STATE OF MARYLAND
ADMINISTRATIVE OFFICE OF THE COURTS
PROCUREMENT, CONTRACT AND GRANT ADMINISTRATION
2003 C COMMERCE PARK DRIVE
ANNAPOLIS, MD 21401

REQUEST FOR PROPOSALS (RFP)

FOR

Emergency Mass and IT Alert Notification System

Project K18-0036-29

ISSUED: October 20, 2017

Sole point of contact for this solicitation is the Procurement Officer. Offerors are specifically directed NOT to contact any other Judiciary personnel or its contracted consultants for meetings, conferences, or discussions that are specifically related to this RFP at any time prior to any award and execution of a contract. Unauthorized contact with any Judiciary personnel or the Judiciary's contracted consultants may be cause for rejection of the Offeror's proposal.

Minority Business Enterprises are encouraged to respond to this Request for Proposals

Procurement, Contract & Grant Administration
http://www.mdcourts.gov

THE JUDICIARY
NOTICE TO OFFERORS/CONTRACTORS

In order to help us improve the quality of Judiciary solicitations, and to make our procurement process more responsive and business friendly, we ask that you take a few minutes and provide comments and suggestions regarding the enclosed solicitation. Please return your comments with your proposals. If you have chosen not to propose on this Contract, please email this completed form to Khrystine.Bunche@mdcourts.gov

Title: Emergency Mass and IT Alert Notification System
Project No: K18-0036-29

1. If you have responded with a "no bid", please indicate the reason(s) below:

( ) Other commitments preclude our participation at this time.
( ) The subject of the solicitation is not something we ordinarily provide.
( ) We are inexperienced in the work/commodities required.
( ) Specifications are unclear, too restrictive, etc. (Explain in REMARKS section.)
( ) The scope of work is beyond our present capacity.
( ) Doing business with Maryland Government is simply too complicated. (Explain in REMARKS section.)
( ) We cannot be competitive. (Explain in REMARKS section.)
( ) Time allotted for completion of the proposals is insufficient.
( ) Start-up time is insufficient.
( ) Insurance requirements are restrictive. (Explain in REMARKS section.)
( ) Proposals requirements (other than specifications) are unreasonable or too risky. (Explain in REMARKS section.)
( ) MBE requirements. (Explain in REMARKS section.).
( ) Prior The Judiciary Contract experience was unprofitable or otherwise unsatisfactory. (Explain in REMARKS section.)
( ) Payment schedule too slow.
Other:_____

2. If you have submitted a proposal, but wish to offer suggestions or express concerns, please use the Remarks section below. (Use reverse side or attach additional pages as needed.)

REMARKS:
_____

Offeror Name: _____

Contact Person: _____ Phone (____) _____ - _____

Address:_____

KEY INFORMATION SUMMARY SHEET

THE JUDICIARY

Request for Proposals

Emergency Mass and IT Alert Notification System

PROJECT # K18-0036-29

RFP Issue Date:	**October 20, 2017**
RFP Issuing Office:	**Procurement, Contract, and Grant Administration**
Procurement Officer:	**Khrystine Bunche** **Maryland Judiciary, Administrative Office of the Court** **Department of Procurement, Contract & Grant Administration** **2003 C Commerce Park Drive** **Annapolis, MD 21401** **410-260-2556** **Khrystine.Bunche@mdcourts.gov**
Proposals must be sent to:	**Khrystine Bunche/K18-0036-29** **Maryland Judiciary, Administrative Office of the Courts** **Department of Procurement, Contract & Grant Administration** **2003 C Commerce Park Drive** **Annapolis, MD 21401**
Pre-Proposal Conference:	**October 30, 2017; 10:00AM** **2003 C Commerce Park Drive** **Annapolis, MD 21401**
Closing Date and Time:	**November 13, 2017; 2:00PM**

A. TABLE OF CONTENTS

SECTION 1 - GENERAL INFORMATION

1.1 Summary Statement

The Administrative Office of the Courts (AOC) issues this Request for Proposals (RFP) to make a single award to procure and implement an Emergency Mass and IT Alert Notification system to replace the AOC's legacy system, RAVE.

1.2 Abbreviations and Definitions

For the purpose of this RFP, the following abbreviations or terms have the meanings indicated below:

a. Contract – The Contract attached to this RFP as Attachment A

b. Contractor– The selected Offerors

c. Local Time – Time in the Eastern Time Zone

d. MBE – Minority Business Enterprise currently so certified by the Maryland State Department of Transportation.

e. Offerors – An entity that submits a proposal in response to this RFP

f. Procurement Officer – The Judiciary representative responsible for this RFP, for the determination of contract scope issues, and the only Judiciary representative who can authorize changes to the contract

g. RFP – Request for Proposals for K18-0036-29 dated October 20, 2017, including any and all amendments.

h. Contract Manager– The Judiciary representative that serves as the technical manager for the resulting contract. The Contract Manager monitors the daily activities of the contract and provides technical guidance to the Contractor.

i. Judiciary business hours – 8:00 am – 5:00 pm Monday – Friday (excluding State holidays and any other days closed by order of the Chief Judge).

j. Service Credit - an amount equal to the daily pro-rata monthly recurring subscription service fee.

k. Active User Account - account with activity in the past 60 days

1.3 Contract Type

The Contract that results from this RFP shall be based on Fixed Firm Price and Time and Materials.

1.4 Contract Duration

The Contract resulting from this RFP shall begin upon execution, and extend for a base period of two years (2 years). The Judiciary shall have the sole right to exercise up to three consecutive one year renewal options at its discretion.

1.5 Procurement Officer

The sole point of contact in the Judiciary for purposes of this RFP prior to the award of any Contract is the Procurement Officer at the address listed below:

Khrystine Bunche
2003 C Commerce Park Drive
Annapolis, MD 21401
410.260.2556
Khrystine.Bunche@mdcourts.gov

The Maryland Judiciary may change the Procurement Officer at any time by written notice to the Contractor .

1.6 Contract Managers

Susan Bowen

The Maryland Judiciary may change the Contract Manager at any time by written notice to the Contractor .

1.7 Pre-Proposal Conference

A Pre-Proposal Conference will be held on October 30, 2017, beginning at 10:00AM, at 2003 C Commerce Park Drive Annapolis, Maryland 21401. Attendance at the Conference is not mandatory, but encouraged in order to facilitate better preparation of proposals.

In order to assure adequate seating and other accommodations at the Conference, please email the Conference Response Form to the attention of the Procurement Officer such notice no later than October 27, 2017 at noon. The Conference Response Form is included as Attachment D to this RFP.

The Conference will be summarized. As promptly as is feasible subsequent to the Conference, that record and all questions and answers known at that time will be posted to the Judiciary's Procurement web site and eMarylandMarketplace.

1.8 Questions

1.8.1 The Procurement Officer shall accept written questions from prospective Offerors. Please submit all questions to the Procurement Officer by e-mail.

1.8.2 The Procurement Officer shall, based on the availability of time to research, communicate a timely answer, beginning with a question-and answer-period during the pre-proposal conference. Answers to all substantive questions and are not clearly specific only to the requestor, will be posted on the Judiciary's Procurement web site and eMarylandMarketplace.

1.9 Proposal Due (Closing) Date

One original and 4 copies of each proposal (technical and financial) must be received by the Procurement Officer **no later than 2:00PM (local time) on October 30, 2017** in order to be considered. An electronic version of the Technical Proposal must be enclosed with the technical proposal. An electronic version of the Financial Proposal must be enclosed with the original Financial Proposal. All electronic versions must be labeled with the RFP title, RFP number, and Offeror name and packaged with the original copy of the appropriate proposal (technical or financial).

Requests for extension of this date or time will not be granted. Offerors mailing proposals should allow sufficient mail delivery time to ensure timely receipt by the Procurement Officer. Proposals received by the Procurement Officer after the due date will not be considered.

Proposals may not be submitted by e-mail or facsimile.

1.10 Duration of Offer

Proposals submitted in response to this RFP are irrevocable for the later of: (1) 180 days following the closing date of proposals or of Best and Final Offers (BAFOs), if requested, or (2) the date any protest concerning this RFP is finally resolved. This period may be extended at the Procurement Officer's request only with the Offerors written agreement.

1.11 Revisions to the RFP

If it becomes necessary to revise this RFP before the due date for proposals, amendments will be posted on the Judiciary's Procurements web page and eMarylandMarketplace. Amendments made after the due date for proposals will be sent only to those Offerors who submitted a timely proposal.

Acknowledgment of the receipt of all amendments to this RFP issued before the proposal due date must accompany the Offerors proposal in the Transmittal Letter accompanying the Technical Proposal submittal. Acknowledgement of the receipt of amendments to the RFP issued after the proposal due date shall be in the manner specified in the amendment notice. Failure to acknowledge receipt of amendments does not relieve the Offeror from complying with all terms of any such amendment.

1.12 Cancellations

The Judiciary reserves the right to cancel this RFP, accept or reject any and all proposals, in whole or in part, received in response to this RFP, to waive or permit cure of minor irregularities, and to conduct discussions with all qualified or potentially qualified Offerors in any manner necessary to serve the best interests of the Judiciary. The Judiciary also reserves the right, in its sole discretion, to award a Contract based upon the written proposals received without prior discussions or negotiations.

1.13 Oral Presentations/Discussions

Offerors may be asked to participate in oral presentations to expand on their proposal**.** We expect to schedule those no later than two weeks after proposal receipt. The Procurement Officer will notify selected Offerors of the time and location.

Significant representations made by an Offerors during the oral presentation shall be submitted in writing. All such representations will become part of the Offerors proposal and are binding if the Contract is awarded.

1.14 Incurred Expenses

The Judiciary will not be responsible for any costs incurred by an Offerors in preparing and submitting a proposal, in making an oral presentation, in providing a demonstration, or in performing any other activities relative to this solicitation.

1.15 Economy of Preparation

Proposals should be prepared simply and economically, providing a straightforward, concise description of the Offerors proposals to meet the requirements of this RFP.

1.16 Protests/Disputes

Any protest or dispute related respectively to this solicitation or the resulting Contract shall be subject to the provisions of the Judiciary's Procurement Policy.

1.17 Multiple or Alternate Proposals

Neither multiple nor alternate proposals will be accepted.

1.18 Public Information Act Notice

An Offeror shall give specific attention to the clear identification of those portions of its proposal that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the Judiciary under the Public Information Act, Title 4, Subtitle 1, Part III of the General Provision Article of the Annotated Code of Maryland or Rules 16-901 through 16-912, the Court Access Rules.

Offerors are advised that, upon request for this information from a third party, the Procurement Officer is required to make an independent determination whether the information can be disclosed. Information which is claimed to be confidential is to be placed after the Title Page and before the Table of Contents in the Technical proposal and if applicable in the Financial proposal.

1.19 Offeror Responsibilities

The selected Offerors shall be responsible for all products and services required by this RFP. All subcontractors must be identified and a complete description of their role relative to the proposals must be included in the Offerors proposals. Additional information regarding MBE subcontractors is provided under paragraph 1.23 below. If an Offerors that seeks to perform or provide the services required by this RFP is the subsidiary of another entity, all information submitted by the Offerors, such as but not limited to, references and financial reports, shall pertain exclusively to the Offerors, unless the parent organization will guarantee the performance of the subsidiary. If applicable, the Offerors

proposal must contain an explicit statement that the parent organization consents to the terms of the RFP and will guarantee the performance of the subsidiary.

1.20 Mandatory Contractual Terms

By submitting an offer in response to this RFP, an Offerors, if selected for award, shall be deemed to have accepted the terms of the Contract, attached as Attachment A. Any exceptions to the terms and conditions of the Contract must be clearly identified in the Executive Summary of the technical proposal. A proposal that takes exception to these terms may be rejected and therefore determined to be not reasonably susceptible of being selected for award.

1.21 Proposal Affidavit

A proposal submitted by an Offeror must be accompanied by a completed Bid/Proposal Affidavit. A copy of this Affidavit is included as Attachment B of this RFP.

1.22 Contract Affidavit

All Offerors are advised that if a Contract is awarded as a result of this solicitation, the successful Offerors will be required to complete a Contract Affidavit. A copy of this Affidavit is included for informational purposes as Attachment C of this RFP. This Affidavit must be provided within five business days of notification of proposed Contract award.

1.23 Minority Business Enterprises

Minority Business Enterprises (MBE) are encouraged to respond to this solicitation notice. It is the goal of the Maryland Judiciary that certified MBEs participate.

There is no MBE Goal established for this solicitation.

1.24 Arrearages

By submitting a response to this solicitation, each Offerors represents that it is not in arrears in the payment of any obligations due and owing the State, including the payment of taxes and employee benefits, and that it shall not become so in arrears during the term of the Contract if selected for Contract award.

1.25 Procurement Method

The Contract resulting from this RFP will be awarded in accordance with the competitive sealed proposals process.

1.26 Verification of Registration and Tax Payment

Before a corporation can do business in the State it must be registered with the Department of Assessments and Taxation, State Office Building, Room 803, 301 West Preston Street, Baltimore, Maryland 21201. It is strongly recommended that any potential Offerors complete the registration prior to the due date for receipt of proposals. An Offerors failure to complete the registration with the

Department of Assessments and Taxation may disqualify an otherwise successful Offerors from final consideration and recommendation for Contract award.

1.27 Payments by Electronic Funds Transfer

By submitting a response to this solicitation, the Offerors agrees to accept payments by electronic funds transfer unless the State Comptroller's Office grants an exemption. The selected Offerors shall register using the COT/GAD X-10 Vendor Electronic Funds (EFT) Registration Request Form. Any request for exemption must be submitted to the State Comptroller's Office for approval at the address specified on the COT/GAD X-10 form and must include the business identification information as stated on the form and include the reason for the exemption. The COT/GAC X-10 form can be downloaded at: http://compnet.comp.state.md.us/gad/pdf/GADX-10.pdf

1.28 Non-Disclosure Agreement

All Offerors are advised that if a contract is awarded as a result of this RFP, the successful Offeror shall be required to complete a Non-Disclosure Agreement. A copy of this Agreement is included for informational purposes as Attachment F of this RFP. This Agreement must be provided within five business days of notification of proposed Contract award.

SECTION 2 – STATEMENT OF WORK

2.1 Purpose & Summary

The purpose of this RFP is to transition from the AOC's current Emergency Mass Notification system, RAVE, and institute emergency conference bridging capabilities as necessary with priority belonging to the replacement of RAVE's functionality.

The Offeror's proposed system shall automate the AOC's IT Alert Notification, on-call support notification, and emergency conference bridging capabilities. Additionally, this RFP requires Implementation Professional Services including:

- Implementation Planning and Execution
- System Configuration
- System Training
- Data Migration (from RAVE and, as appropriate from Active Directory and ServiceNow)
- Project Management

2.2 Statement of Work – System Requirements

2.2.1 System Environments

Contractor shall provide at least two (2) separate System Environments for use by AOC/JIS including:

- Production Environment
- System Development, Test Environment and Stage/Pre-Production Environment

The System must be currently installed and providing SaaS support in at least five (5) separate entities, with at least two (2) installations that support at least 5000 Users.

2.2.2 System Environment Capabilities

Contractor shall provide the following capabilities to migrate data, account information, and manage system configurations between System Environments:

- The ability to create, name, store and apply different System configurations to enable rapid and repeatable application of specific system configurations to one or more environments
- The ability to migrate configuration settings from one System Environment to another
- The ability to migrate user accounts, customer profiles, groups, table, and security settings from one System environment to another

- The ability to migrate data from one System Environment to another
- The ability to import and export data from a System Environment to and from other external systems.
- The ability to report active user accounts.

2.2.3 Subscription Service

The Subscription Service described below is intended to afford AOC/JIS the ability to add User Accounts as required.

- AOC's legacy system currently has approximately 50 Users.
- New subscriptions shall be invoiced on a pro-rated basis through the end of the Contract Year based on active User Accounts, (active User Account herein defined as a user account with activity in the past 60 days) in the Production Environment. This maintains all licenses to terminate at the end of the then-current contract year.
- Active User Accounts shall be determined as of the last day of the Contractor's monthly billing cycle and documented in a Monthly Active User Report providing the account names and total count of all active users. Additional subscriptions will be added if the number of Active Users is more than for the prior month.
- The Contractor shall allow AOC to reduce subscription counts at the beginning of the next Contract Year as part of an annual Subscription synchronization. Subscription count will not go below 75 users for any contract year.
- Contractor shall provide with its invoice a copy of the report showing the number of active users and the date the report was run.

2.2.4 System Operational Support Services

The Contractor is responsible for ensuring that System Operational Support Services are provided by the Contractor and Cloud Service Provider in accordance with the AOC negotiated between the Cloud Service Provider and AOC. The costs for System Operational Support Services shall be included in the Subscription Price.

System Operational Support Services consist of:

- A Service Support Manual that outlines support services processes that the Cloud Service Provider and AOC shall follow to achieve service support for the System. This document will outline all contact, escalation and remediation processes used to support the System.

- Cloud Service Provider's service desk shall be available by telephone web site and e-mail on a 24 hour basis, 365 days per year commencing at the time that the first System Environment is accessible by AOC.

- Responding to all System service interruptions in accordance with the Service Level Agreement (SLA)

- Responding to all requests from designated AOC personnel for assistance with respect to the System.

- Performing all support services required to maintain System uptime in accordance with the SLA requirements

- Providing services to ensure that data is secured, protected and managed in accordance with the JIS Information Security Policy.

- Performing all service functions and software upgrades necessary to ensure that the System is operating in compliance with all functional and non-functional requirements

2.2.5 Service Level Agreement

The Service Levels provided below are applicable to all service support provided by the Contractor in support of the System. Service levels are defined as follows:

- Urgent: Any incident, issue or problem which results in an inability to use the System as designed by 10 or more Users, and for which there is no acceptable workaround solution
- High: Any incident that prevents one or more Users from accessing or using the System or 5 or more Users who are prevented from using one or more functions of the System
- Normal: Routine issues and problems which do not directly impact any User's ability to access and use the System.

Response and Remediation SLA			
Service Levels	Response	Problem resolution or escalation	Response Availability
Urgent	15 minutes by phone 24X7 to the AOC Primary and/or Secondary contacts.	1 hour	7 days/week, 24 hrs. a day
High	1 hour by phone/e-mail 24/7 to the AOC Primary and/or Secondary contacts.	4 hours	7 days/week, 24 hrs. a day
Normal	1 hour by phone/e-mail Primary and/or Secondary contacts during working hours.	1 work day	5 days/week, Mon-Fri, 8AM-5PM

2.2.6 Availability SLA

The Cloud Software Provider shall provide availability of 99.9% for each month of the awarded contract and any extensions thereto excluding pre-scheduled maintenance. The CSP shall document and provide its maintenance policies and pre-scheduled maintenance windows as part of the Service Support Manual. The CSP shall document and adhere to its published SLAs to include:

- Monthly Service Availability (Measured as total availability hours / Total hours within the month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.9%)
- Within 24 hours of an Urgent outage occurrence resulting in greater than 1-hour of unscheduled downtime: The CSP shall provide a root cause analysis and describe actions taken to remediate the problem.
- Routine maintenance windows shall be scheduled at least one week in advance, and require notification to the AOC/JIS primary or secondary point of contract.
- Pre-scheduled routine maintenance shall not be performed during the period from 7:00 AM to 7:00 PM during weekdays excluding State holidays, State Furlough Days and State Reduction Days.
- New Releases of the System shall be scheduled at least two weeks in advance, require notification to the AOC/JIS primary or secondary point of contact and require that the CSP provide, via pre-release notes, documented impact and test results that describe the changes that are being made to the System.

The CSP's Service Level Agreements (SLAs) shall not be changed except as approved by the Contract Manager.

2.2.7 Service Credits in the Event of Deficiencies in Meeting SLAs

A **Service Credit** is an amount equal to the daily pro-rata monthly recurring subscription service fee. One Service Credit equals one (1) calendar day of subscription service for all subscriptions.

It is critical to the success of this Contract that services be maintained in a timely manner and that the Contractor operates in an extremely reliable manner. It would be impracticable and extremely difficult to fix the actual damage sustained by AOC in the event of certain delays or failures in administration and provision of services under this Contract. In the event that SLAs discussed in this section are not achieved and that the failure is attributable to the Contractor or third parties working on behalf of the Contractor, Service Credits will be issued to AOC by the Contractor.

2.2.8 Remedies

System Availability - AOC shall receive a Service Credit if it experiences performance issues in which System Availability (measured in a calendar month) is less than 99.9% and the source of the performance issue is within the sole control of the Contractor as determined by the description of the outage, the root cause analysis provided by the Contractor and the judgment of the Contract Manager.

Continuous Downtime in Excess of 120 Minutes - AOC shall receive a Service Credit if it experiences performance issues in which System Availability is unavailable for a continuous period that exceeds 120 minutes and the source of the performance issue is within the sole control of the Contractor

Service Credits must be initiated by AOC - In order to receive any of the Service Credits described, AOC must notify the Contractor in writing within ninety (90) days from the occurrence of any event for which Service Credit(s) are the remedy.

Maximum Service Credits - In the event that AOC experiences downtime, in other than a catastrophic event, it shall be eligible to receive from the Contractor a Service Credit. The aggregate maximum number of Service Credits to be issued by the Contractor in a single calendar month shall not exceed fifteen (15) Service Credits.

2.3 Statement of Work - Professional Services

The Offeror must propose Professional Services, which are required by the AOC to transition from RAVE. The period of performance for this task will be limited to three (3) months. If additional services are required, AOC will request a statement of work detailing the services and deliverables and modify the contract accordingly.

2.3.1 Labor Category – Subject Matter Expert, SME:

SME shall oversee configuration, implementation, training, and the transition of operation to the System. The SME is considered to be key personnel for the Contract. The SME shall be responsible for the following activities:

- Serve as a subject matter expert on the configuration and best practice usage of the System
- Assist AOC in configuring the System to meet AOC's needs.
- Plan the implementation and transition process to include the initial entry or migration of data
- Provide training to staff in the creation and editing of new business processes.
- Submit a bi-weekly Status Report to the Contract Manager and/or hold a bi- weekly status meeting to discuss the status of the System

The SME shall perform work in AOC offices in Annapolis.

Status Reports of SME

Status Reports shall be bi-weekly or as required by the Contract Manager and shall contain the following information:

1. Status all tasks to have been completed in the reporting period.
2. Status any milestones from previous reporting periods that have not been achieved.
3. Tasks that due to be completed in the next reporting period.
4. Review the issue and risk log (status on all current issues).
    - Add new items discovered during the reporting period.
    - Updated resolutions and actions taken during the reporting period
5. Integrated schedule updated and embedded in status report

Status meetings shall be held following delivery of the Status Report to discuss the contents of the report and any other open issues.

2.4 Project Management

2.4.1 The Project Management requirements include the following major tasks:

- Task 1 - Project Initiation

- Task – 2 Project Management Plan (PMP) to include the following subsidiary planning documents:
    - Project Scope Statement
    - Project Schedule
    - Project Communication Management Plan
    - Project Stakeholder Management Plan
    - Implementation Plan
    - Project Risk Register

- Task 3 - Meeting Requirements
  - Agendas
  - Meeting Minutes

- Task 4 - Status Reporting

- Task 5 - Issues Management

2.4.2 The Contractor shall perform the following tasks to fulfill the Project Management requirements of this TORFP:

2.4.2.1 Task 1 – Project Initiation

Performance Objectives
The contractor shall designate their Project Team to include a Project Manager and key personnel. The contractor shall provide the necessary staff resources to participate in the project initiation kick off meeting.

Measurable Benefits/Improvements/Outcomes
Measurable outcomes are to provide the Judiciary with a project agenda that contains project specific discussion points at least three days prior to the kickoff meeting. The contractor shall identify and introduce the key personnel composing the Project Team. The contractor shall ensure that key personnel, including the contractor's Project Manager, participate in a kick-off meeting to present the contractor's overall approach to completing the tasks defined in this TORFP. The contractor shall document the decisions, action items, responsibility for completing each action item and the procedure for tracking the resolution of all action items identified during the kick-off meeting using a format proposed by the Judiciary.

2.4.2.2 Task 2 - Project Planning

Performance Objectives
This task will result in the development of detailed PMP that will be used as the basis for performing Tasks. The contractor shall review the PMP documents and provide a rough order of magnitude estimate to complete the PMP. The PMP discussion will focus on the following subsidiary documents: Project Schedule, Communication and Stakeholder Management Plans, Implementation Plan and Project Risk Register. The contractor shall utilize JIS templates to create the PMP. The templates for these documents are located at:
http://doit.maryland.gov/SDLC/Pages/PDFDownloads.aspx.

Measureable Benefits/Improvements/Outcome
The contractor shall use the high level requirements identified in the RFP to develop the PMP for implementation of the solution for the Emergency Mass and IT Alert Notification System. The contractor shall use Microsoft project to create the project

schedule containing both the Judiciary's and the contractor's work activities. The Contractor's Project Schedule shall take into account State holidays and service reduction days. The contractor shall utilize Microsoft Word to create the PMP.

2.4.2.3 Task 3 – Meeting Requirements

Performance Objective
The objective of this task is to ensure the contractor produces an agendas and meeting minutes for all project team meetings. The agenda serves as a notice of a meeting.

Measurable Benefits/Improvements/Outcomes
The contractor shall produce a meeting agenda for all meetings using the template provided by the Judiciary. The agenda shall contain a list of items/topics to be discussed during the meeting. The meeting agenda shall be emailed to the project team at least two days prior to the meeting. The agenda enables meeting participants to prepare in advance for the topics so that they can make a more valuable contribution to the meeting.

Performance Objective
The objective of this tasks is to make certain the contractor produces Meeting Minutes.

Measurable Benefits/Improvements/Outcomes/Improvements
The contractor shall produce meeting minutes for all meetings. The meeting minutes will record action points/items, who is responsible and the milestones and deadlines that are impacted by the action points. The meeting minutes record summaries of the discussions held at the meeting.

2.4.2.4 Task 4 – Status Reporting

Performance Objective
The contractor shall provide a weekly status report using the template provided by the Judiciary.

Measurable Benefits/Improvements/Outcomes/Improvements
The contractor shall produce a weekly status report. The status report is a formalized report on the project progress against the project schedule. It will effectively and efficiently communicate project status. The status report will be used to provide a documented history of the project.

2.4.2.5 Task 5 – Issues Management

Performance Objective
The purpose of this Task is to ensure the contractor produces an issues log using the template provided by the Judiciary.

Measurable Benefits/Improvements/Outcomes/Improvements
The contractor shall produce an issue log on a weekly basis. Review of the issues log will be a major component of the status meetings. The issues log will be used to manage the ongoing and closed issues.

2.5 Acceptance of Services and Deliverables

2.5.1 The AOC or designated representative has sole authority to determine acceptable level of service.

2.5.2 When the AOC or designee determines that Contractor service is unsatisfactory, the Contractor shall return to the site at the request of the AOC, or an authorized designee and resolve the issue at no additional cost to the AOC.

2.5.3 For each written deliverable, draft and final, the contractor shall submit to the AOC's Project Manager one hard copy and one electronic copy.

Drafts of all written deliverables are required no later than one week in advance of when the final deliverable is due. Written deliverables identified as draft must demonstrate due diligence in meeting the scope and requirements of the associated final written deliverable. A draft deliverable may contain limited structural errors such as poor grammar, misspellings or incorrect punctuation, but must:

- Be presented in a format appropriate for the subject matter and depth of discussion.
- Be organized in a manner that presents a logical flow of the deliverable's content.
- Represent factual information reasonably expected to have been known at the time of submittal.
- Present information that is relevant to the Section of the deliverable being discussed.
- Represent a significant level of completeness towards the associated final written deliverable that supports a concise final deliverable acceptance process.

Upon receipt of a final deliverable, the Project Manager shall commence a review of it to validate its completeness, quality and response to requirements. Upon completion of this review, the Project Manager shall obtain the signatures of Project Sponsor and Project Business Owner as notice of acceptance or rejection of the deliverable. In the event that the deliverable is rejected, the contractor shall correct the identified deficiencies or non-conformities. Subsequent project tasks may not continue until the deficiencies in the deliverable are rectified and accepted by the Project Manager, unless the Project Manager issues a written waiver for conditional continuance of project tasks. Once the Project Manager's issues have been addressed and resolutions are accepted by the Project Manager, the contractor will incorporate the resolutions into the deliverable and resubmit it for acceptance.

The State required deliverables are defined below. Within each task, the contractor may suggest other subtasks or deliverables to improve the quality and success of the project.

2.5.4 Deliverables:

Task 1 - Project Initiation

Agenda and Meeting Minutes – The contractor shall participate in a Project Kick-off Meeting as specified in TORFP.

Deliverable(s) - The contractor shall produce a project kickoff meeting agenda detailing discussion points. The Agenda shall contain the list of topics that will be discussed during the meeting. This tool enables participants to prepare in advance for the topics so that they can make a more valuable contribution to the meeting. The Agenda shall be provided to the Project Manager at least three business days prior to the start of the meeting. The contractor shall document the Meeting Minutes using Microsoft Word in a format proposed by the Project Manager within three business days of the end of the meeting. The Meeting Minutes serves to record action points, who is responsible and what the milestones and deadlines are. Additionally, Meeting Minutes also record summaries of the discussions held at the meeting. Both the Agenda and Meeting Minutes shall be produced using Microsoft Word.

Task 2 – Project Planning

Project Management Plan (PMP) - The contractor shall develop a detailed PMP containing the subsidiary plans as specified in TORFP using the State SDLC templates located at: (http://doit.maryland.gov/SDLC/Pages/Templates.aspx).

Deliverable(s) - Presentation of the Project Management Plan (Microsoft Word) containing the following subsidiary plans: Scope statement, Communication and Stakeholder Management Plans, Implementation Plan and Risk Register. For the Emergency Mass and IT alert Notification system, the project shall be divided into two unique phases. Phase 1 shall replace the current system (RAVE) functionality and Phase 2 shall include all remaining functionality. Both the Implementation Plan and the Project Schedule should reflect these requirements.

Deliverable(s) - Project Schedule - The contractor shall develop a Project Schedule as specified in TORFP using the template provided by the Judiciary. The Project Schedule is the time-sequenced plan of activities or tasks used to direct and control project execution. The project schedule contains at a minimum: WBS number, task name, durations (days), work (hours), predecessor, successor, estimated start and finish, actual start and finish, resource name and percent complete.

Task 3 – Meeting Requirements – The contractor shall create an Agenda and Meeting Minutes for all meetings.

Deliverable(s) - The Agenda shall contain the list of topics that will be discussed during the meeting. This tool enables participants to prepare in advance for the topics so that they can make a more valuable contribution to the meeting. The Agenda shall be provided to the Project Manager at least three business days prior to the start of the

meeting. The contractor shall document the Meeting Minutes using Microsoft Word in a format proposed by the Judiciary within three business days of the end of the meeting. The Meeting Minutes serve to record action points, who is responsible and what the milestones and deadlines are. Additionally, Meeting Minutes also record summaries of the discussions held at the meeting. Both the Agenda and Meeting Minutes shall be produced using Microsoft Word.

Task 4 - Status Reporting - The contractor shall produce a weekly Status Report.

Deliverable(s) - The contractor shall email the Judiciary's Project Manager a status report on a weekly basis. This tool will ensure the objectives of the project are being met by monitoring and measuring progress regularly to determine variances from the project schedule. The contractor shall use the template provided by the Judiciary to produce the weekly status report.

Task 5 – Issues Management – The contractor shall produce an Issues Log.

Deliverable(s) - The contractor shall create an issues log to monitor elements under discussion or dispute between project stakeholders. It contains a list of all open action points/items that require resolution. Along with each issue, the log shall also contain the person or people responsible for resolving the issue.

2.6 Failure to Respond

2.6.1 Should the Contractor fail to respond to the request for service as specified herein, the Judiciary may, at its option, directly or by contract, take whatever measures are necessary to provide the necessary services at the expense of the Contractor. Such expense incurred shall be deducted directly from the Contractor's monthly invoice.

CONTRACTOR DUTIES AND RESPONSIBILITIES

The Contractor shall be responsible for providing on a continual basis staff as awarded for all assigned tasks as described in Section 2, the personnel required in this RFP within the timeframe required as specified.

Licensed and/or copyrighted data shall be governed by the terms and conditions identified in the Contract.

REQUIRED POLICIES, GUIDELINES AND METHODOLOGIES

The Contractor shall be required to comply with all applicable laws, regulations, policies, standards and guidelines affecting information technology projects, which may be created or changed periodically by JIS and/or the State of Maryland.. The Contractor shall adhere to and remain abreast of current, new, and revised laws, regulations, policies, standards and guidelines affecting project execution. These may include, but are not limited to:

- The State's System Development Life Cycle (SDLC) methodology

- The State Information Technology Security Policy and Standards
- The Judiciary's new Enterprise Architecture

2.7 Contractor Security Requirements

Compliance with Judiciary Policies-
-The Contractor, and all contractor and subcontractor personnel assigned to the Contract (contractor personnel), shall comply with all applicable Judiciary policies and procedures, as provided by the Judiciary Contract Manager (JCM), for the duration of the contract.

Security requirements are detailed in Attachment H.

2.8 Insurance

2.8.1 The Contractor shall at all times during the term of the Contract maintain in full force and effect, the policies of insurance required by this Section. Evidence that the required insurance coverage has been obtained may be provided by Certificates of Insurance duly issued and certified by the insurance company or companies furnishing such insurance. Such evidence of insurance must be delivered to the AOC Office of Procurement before the actual implementation of the Agreement.

2.8.2 All insurance policies shall be endorsed to provide that the insurance carrier will be responsible for providing immediate and positive notice to the AOC in the event of cancellation or restriction of the insurance policy by either the insurance carrier or the Contractor, at least 60 days prior to any such cancellation or restriction. All insurance policies shall name as an additional insured the Administrative Office of the Courts and the Maryland Judiciary.

2.8.3 The limits required below may be satisfied by either individual policies or a combination of individual policies and an umbrella policy. The requiring of any and all insurance as set forth in this RFP, or elsewhere, shall be in addition to and not in any way in substitution for all the other protection provided under the Contract.

No acceptance and/or approval of any insurance by AOC, or the Manager of Procurement, shall be construed as relieving or excusing the Contractor from any liability or obligation imposed upon it by the provisions of the Contract.

A. The Contractor shall maintain Worker's Compensation insurance as required by the laws of the State of Maryland and including Employer's Liability coverage with a minimum limit of $500,000-each accident; $500,000 disease-each employee; and $500,000 disease-policy limit.

B. Occurrence forms of comprehensive general liability insurance covering the full scope of this agreement with limits not less than $1,000,000 per occurrence and $2,000,000 aggregate for personal or bodily injuries and $1,000,000 per occurrence

and aggregate for property damage. A combined single limit per occurrence of $2,000,000 is acceptable. All policies issued shall include permission for partial or total occupancy of the premises by or for the Administrative Office of the Courts within the scope of this Contract. Such insurance shall include but shall not be limited to, the following:

C. Comprehensive general liability insurance including a comprehensive broad form endorsement and covering: a) all premises-operations, b) completed operations, c) independent Contractors, d) liability assumed by oral or written contract or agreement, including this contract, e) additional interests of employees, f) notice of occurrence, g) knowledge of occurrence by specified official, h) unintentional errors and omissions, i) incidental (contingent) medical malpractice, j) extended definition of bodily injury, k) personal injury coverage (hazards A and B) with no exclusions for liability assumed contractually or injury sustained by employees of Contractor, l) broad form coverage for damage to property of the Administrative Office of the Courts, as well as other third parties resulting from completion of the Contractor's services.

D. Comprehensive business automobile liability insurance covering use of any motor vehicle to be used in conjunction with this contract, including hired automobiles and non-owned automobiles.

E. Comprehensive Automobile Liability:

Limit of Liability - $1,000,000 Bodily Injury
$1,000,000 Property Damage

In addition to owned automobiles, the coverage shall include hired automobiles and non-owned automobiles with the same limits of liability.

2.8.4 The insurance required under sub-paragraphs (A),(B), (C) and (D) above shall provide adequate protection for the Contractor against claims which may arise from the Contract, whether such claims arise from operations performed by the Contractor or by anyone directly or indirectly employed by him, and also against any special hazards which may be encountered in the performance of the Contract. In addition, all policies required must not exclude coverage for equipment while rented to others.

2.8.5 If any of the work under the Contract is subcontracted, the Contractor shall require subcontractors, or anyone directly or indirectly employed by any of them, to procure and maintain the same coverages in the same amounts specified above.

SECTION 3 – PROPOSAL FORMAT

3.1 Two Part Submission

3.1 Offerors must submit proposals in two separate volumes:

- Volume I - TECHNICAL PROPOSAL
- Volume II - FINANCIAL PROPOSAL

3.2 Proposals

3.2.1 Volume I-Technical Proposal, must be sealed separately from Volume II-Financial Proposal, but submitted simultaneously to the Procurement Officer (address listed in Section 1.5 of this RFP).

3.2.2 Submit (1) one unbound original, so identified, and (4) four copies of each volume are to be submitted. An electronic version of both the Volume I- Technical Proposal and the Volume II- Financial Proposal must also be submitted originals technical or financial volumes, as appropriate.

3.2.3 Electronic media shall bear a label with the RFP title and number, name of the Offerors, and the volume number (I or II).

3.3 Submission

3.3.1 Each Offerors is required to submit a separate sealed package for each "Volume", which is to be labeled Volume I-Technical Proposal and Volume II-Financial Proposal, respectively. Each sealed package must bear the RFP title and number, name and address of the Offerors, the volume number (I or II), and the closing date and time for receipt of the proposals on the outside of the package.

3.3.2 All pages of both proposal volumes must be consecutively numbered from beginning (Page 1) to end (Page "x").

3.4 Volume I – Technical Proposal

3.4.1 Transmittal Letter: A transmittal letter must accompany the technical proposal. The purpose of this letter is to transmit the proposal and acknowledge the receipt of any addenda. The transmittal letter shall be brief and signed by an individual who is authorized to commit the Offerors to the services and requirements as stated in this RFP. Only one transmittal letter is needed and it does not need to be bound with the technical proposal.

3.4.2 Format of Technical Proposal: Inside the sealed package described in Section 3.3, above, an unbound original, to be so labeled, four copies and one electronic version shall be enclosed. Section 2 of this RFP provides requirements and Section 3 provides reply instructions. The paragraphs in these RFP sections are numbered for ease of reference. In addition to the instructions below, the Offerors technical proposals shall be organized and numbered in the same order as this RFP. This proposal organization shall allow Judiciary officials and the Evaluation Committee to "map" Offerors responses directly to RFP requirements by paragraph number. The technical proposal shall include the following sections in the stated order:

3.4.3 Title and Table of Contents: The technical proposal shall begin with a title page bearing the name and address of the Offerors and the name and number of this RFP. A table of contents for the technical proposal should follow the title page. Note: Information that is claimed to be confidential under RFP Section 1.18 is to be printed on yellow paper and placed after the Title Page and before the Table of Contents in the Offerors Technical Proposal, and if applicable, also in its Financial Proposal. Unless there is a compelling case, an entire proposal should not be labeled confidential but just those portions that can reasonably be shown to be proprietary or confidential.

3.4.4 Executive Summary: The Offerors shall condense and highlight the contents of the technical proposal in a separate section titled "Executive Summary." The summary shall also identify any exceptions the Offerors has taken to the requirements of this RFP, the Contract (Attachment A), or any other attachments. Exceptions to terms and conditions may result in having the proposal deemed unacceptable or classified as not reasonably susceptible of being selected for award. If an Offeror takes no exception to the Judiciary's terms and conditions, the Executive Summary should so state.

3.4.5 Offerors Technical Response to RFP Requirements:

3.4.5.1 General

Offerors shall address each RFP requirement in the Technical Proposal and describe how its proposed services will meet those requirements. If the Judiciary is seeking Offerors agreement to a requirement, the Offerors shall state agreement or disagreement. Any paragraph that responds to a work requirement shall not merely rely on a stated agreement to perform the requested work; but rather, the Offerors should outline how the Offerors can fulfill the requested tasks in a manner that best meets the Judiciary's needs.

3.4.5.2 Offerors Experience and Capabilities: Offerors shall include information on past experience with similar engagements. Offerors shall describe their experience and capabilities through a response to the following:

- An overview of the Offerors experience providing the services. (additional items if needed, plans, timelines, etc.)

3.4.5.3 References. Provide three **(3)** current customer references where the customer is similar in size to the RFP scope . Provide the following information for each client reference:

- Name of Client Organization
- Name, title, and telephone number of Point-of-Contact for client organization
- Value, type, and duration of contract(s) supporting client organization
- The services provided, scope of the contract, and number of employees serviced

3.4.5.4 Financial Capability and Insurance: The Offerors shall include the following, for itself, and, as applicable, for any parent corporate, subsidiary is preference under RFP Section 1.19:

- Evidence that the Offeror has the financial capacity to provide the goods and/or services, as described in its proposal, via profit and loss statements and balance sheets for the last two years.
- A copy of the Offerors current applicable certificate of insurance (property, casualty and liability), which, at a minimum, shall contain the following:
  - Carrier (name and address)
  - Type of insurance
  - Amount of coverage
  - Period covered by insurance
  - Exclusions

3.4.5.5 Subcontractors: Offerors must identify non-MBE subcontractors, if any, and the role these subcontractors shall have in the performance of the Contract.

3.4.5.6 Required Affidavits, Schedules and Documents to be submitted by Offerors in the Technical Proposal:

- Completed Bid/Proposal Affidavit (Attachment B – with original of Technical Proposal)
- Copy of insurance to AOC. By submitting a proposal in response to this solicitation, the offerors warrants that it is able to provide evidence of insurance required by RFP Section 2.

3.5 Volume II - Financial Proposal

3.5.1 Under separate sealed cover from the Technical Proposal and clearly identified with the same information noted on the Technical Proposal, the Offerors must submit an original unbound copy, four copies and one electronic copy of the Financial Proposal in a separate envelope labeled as described in Section 3.3, of the Financial Proposal. The Financial Proposal must contain all price information in the format specified in Attachment E. Information which is claimed to be confidential is to be clearly identified in the Offerors Financial Proposal. An explanation for each claim of confidentiality shall be included as part of the Financial Proposal.

The Contractor will not be reimbursed for any travel expenses including but not limited to transportation, meals, hotel accommodations except as approved in advance by the AOC CM.

SECTION 4 – EVALUATION CRITERIA AND SELECTION PROCEDURE

4.1 Evaluation Criteria

4.1.1 Evaluation of the proposals shall be performed by a committee organized for the purpose of analyzing the technical proposals. Evaluations shall be based on the criteria set forth below. The Contract resulting from this RFP shall be awarded to the Offerors that is most advantageous to the Judiciary, considering price and the evaluation factors set forth herein. In making this determination, technical factors shall receive greater weight than price factors.

4.1.2 The Offerors shall be evaluated on the proposed services according to the specifications outlined in this RFP.

4.2 Technical Criteria

4.2.1 The criteria to be applied to each technical proposal are listed in descending order of importance

- Offerors experience and capabilities, including references
- Technical response to requirements of RFP Section 2

4.3 Financial Criteria

All qualified Offerors will be ranked from the lowest to the highest price based on their total price proposed on Attachment E – Price Proposal.

4.4 Selection Process and Procedures

4.4.1 General Selection Process:

4.4.1.2 The Contract shall be awarded in accordance with the competitive sealed proposals process under the Judiciary's Procurement Policy. The competitive sealed proposals method is based on discussions and revision of proposals during these discussions.

4.4.1.3 Accordingly, the Judiciary may hold discussions with all Offerors judged reasonably susceptible of being selected for award, or potentially so. However, the Judiciary also reserves the right to make an award without holding discussions. In either case of holding discussions or not doing so, the Judiciary may determine an Offeror to be not responsible and/or not reasonably susceptible of being selected for award, at any time after the initial closing date for receipt of proposals and the review of those proposals.

4.4.2 Selection Process Sequence:

4.4.2.1 The first level of review shall be an evaluation for technical merit by the selection committee. During this review, oral presentations and discussions may be held. The purpose of such discussions shall be to assure a full understanding of the Judiciary's requirements and the Offerors ability to perform, and to facilitate understanding of the Contract that shall be most advantageous to the Judiciary.

4.4.2.2 Offerors must confirm in writing any substantive oral clarifications of, or changes in, their proposals made in the course of discussions. Any such written clarification or change then becomes part of the Offerors proposal.

4.4.2.3 The financial proposal of each Offeror shall be evaluated separately from the technical evaluation. After a review of the financial proposals of Offerors, the Procurement Officer may again conduct discussions.

4.4.2.4 When in the best interest of the Judiciary, the Procurement Officer may permit Offerors who have submitted acceptable proposals to revise their initial proposals and submit, in writing, best and final offers (BAFOs).

4.4.2.5 Upon completion of all discussions and negotiations, reference checks, and site visits, if any, the Procurement Officer shall recommend award of the Contract to the responsible Offerors whose proposal is determined to be the most advantageous to the Judiciary considering evaluation and price factors as set forth in this RFP. In making the most advantageous Offerors determination, technical shall be given greater weight than price factors.

ATTACHMENTS

Attachment A	Contract
Attachment B	Bid/Proposal Affidavit
Attachment C	Contract Affidavit
Attachment D	Pre-Proposal Conference Form
Attachment E	Price Proposal Form
Attachment F	Non-Disclosure Agreement
Attachment G	HR Background Consent Form
Attachment H	General Requirements Form

ATTACHMENT A – STANDARD CONTRACT AGREEMENT

MARYLAND ADMINISTRATIVE OFFICE OF THE COURTS
STANDARD TERMS AND CONDITIONS
EMERGENCY MASS AND IT ALERT NOTIFICATION SYSTEM
CONTRACT NUMBER: K18-0036-29

This Contract is made this _____ day of _____ 2017, by and between the Administrative Office of the Courts (the "AOC") in the State of Maryland and (Company Name), (Company Address) (the "Contractor") with Federal Taxpayer Identification Number XX-XXXXXXX.

In consideration of the mutual covenants and promises herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the AOC and the Contractor agree as follows:

1. Scope of Contract

1.1 The Contractor shall provide an Emergency Mass and IT Alert Notification System (hereinafter "Goods" or "Services"), and other deliverables in accordance with the terms and conditions of this Contract and the following Exhibits, which are attached to this Contract and incorporated as part of this Contract:

Exhibit A: Contract Affidavit

Exhibit B: Request for Proposal dated October 20, 2017 and all amendments and exhibits thereto (collectively referred to as the "RFP")

Exhibit C: Contractor's Proposal dated **(Contractors Proposal Date)** and any subsequent BAFO dated **(BAFO Date)** (collectively referred to as "the Proposal")

1.2 If there are any inconsistencies between the contract and any of the Exhibits, the terms of this Contract shall prevail. If there are any inconsistencies between Exhibit B and Exhibit C, Exhibit B shall prevail.

1.3 No other order, statement, or conduct of the Procurement Officer or of any other person shall be treated as a change or entitle the Contractor to an equitable adjustment under this section. Any modification to this Contract must first be approved in writing by the Procurement Officer, subject to any additional approvals required by State law and the Maryland Judiciary's Procurement Policy and procedures.

1.4 Except as otherwise provided in this Contract, if any order causes an increase or decrease in the Contractor's cost of, or the time required for, the performance of any part of the work, an equitable adjustment in the Contract price shall be made and the Contract modified in writing

accordingly. The Contractor must assert in writing its right to an adjustment under this section within thirty (30) days of receipt of a written change order and include a written statement setting forth the nature and cost of such claim. No claim by the Contractor shall be allowed if asserted after final payment under this Contract.

1.5 Failure to agree to an adjustment under this section shall be a dispute under the Disputes clause. Nothing in this section shall excuse the Contractor from proceeding with the Contract as changed.

2. <u>Term of the Contract</u>

Unless the Contract is terminated earlier as provided herein, the term of the Contract is the period of (3) years beginning at the execution date of the contract. The AOC, at its sole option, shall have the unilateral right to extend the contract for up to two (2), years(s) renewal options at its discretion. Audit, confidentiality, document retention, and indemnification obligations under this Contract shall survive the expiration or termination of the Contract.

3. <u>Consideration and Payment</u>

3.1 In consideration of the satisfactory performance of the Services, the AOC shall pay the Contractor in accordance with the terms of this Contract and at the rate specified in the Request for Proposal. Except with the express written consent of the Procurement Officer, total payments to the Contractor pursuant to the original form of this Contract may not exceed **$.....** (the "NTE Amount").

3.2 All invoices shall be submitted within thirty (30) calendar days after the completion and acceptance by the AOC for each deliverable and include the following information: name and address of the AOC; vendor name; remittance address; federal taxpayer identification or (if owned by an individual) his/her social security number; invoice period; invoice date; invoice number; amount due; and the deliverable ID number for the deliverable being invoiced. Additional information may be required in the future. Invoices submitted without the required information will not be processed for payment until the Contractor provides the requested information.

3.3 Payments to the Contractor for each deliverable should be made no later than thirty (30) days after the acceptance of the deliverable and receipt of a proper invoice from the Contractor. Charges for late payment of invoices are prohibited.

3.4 In addition to any other available remedies, if, in the opinion of the Procurement Officer, the Contractor fails to perform in a satisfactory and timely manner, the Procurement Officer may refuse or limit approval of any invoice for payment and may cause payments to the Contractor to be reduced or withheld until such time as the Contractor meets performance standards as established by the Procurement Officer in accordance with this Contract. Final payment shall not be construed as a waiver or termination of any rights and remedies available to AOC for any failure of Contractor to perform the Contract in a satisfactory and timely manner.

4. Warranties

The Contractor hereby represents and warrants that:

4.1 It is qualified to do business in the State of Maryland and that it will take such action as may be necessary to remain so qualified;

4.2 It shall comply with all federal, State and local laws applicable to its activities and obligations under this Contract;

4.3 It shall obtain, at its expense, all licenses, permits, insurance, and governmental approvals, if any, necessary to the performance of its obligations under this Contract; and

4.4 It is responsible for all acts and omissions of its agents, employees, and subcontractors, including, but not limited to violations of the Non-Disclosure Agreement.

5. Patents and Copyrights, if applicable

5.1 If the Contractor furnishes any design, device, material, process, code, or other item that is covered by a patent or copyright or which is proprietary to or a trade secret of another, the Contractor shall obtain the necessary permission or license for the AOC's use of such item or items.

5.2 The Contractor shall defend or settle, at its own expense, any claim or suit against the State, AOC, or their employees acting within the scope of employment, alleging that any such item furnished by the Contractor infringes any patent, trademark, copyright, or trade secret. The Contractor also shall pay all damages and costs that by final judgment might be assessed against the State, AOC, or their employees acting within the scope of employment, due to such infringement and all attorney fees and costs incurred by the State to defend against such a claim or suit.

5.3 If any products furnished by the Contractor become, or in the Contractor's opinion are likely to become, the subject of a claim of infringement, the Contractor shall, at its option and expense: a) procure for the AOC the right to continue using the applicable item, b) replace the product with a non-infringing product substantially complying with the item's specifications, or c) modify the item so that it becomes non-infringing and performs in a substantially similar manner to the original item.

5.4 If the Contractor obtains or uses for purposes of this Contract any design, device, material, process, code, supplies, equipment, text, instructional material, services or other work, the Contractor shall indemnify the AOC, its officers, agents, and employees with respect to any claim, action, cost, or judgment for patent, trademark, or copyright infringement, arising out of the possession or use of any design, device, material, process, supplies, equipment, text, instructional material, services or other work covered by any Contract awarded.

6. Non-hiring of Employees

No employee of the Maryland Judiciary or any unit hereof whose duties as such employee include matters relating to or affecting the subject matter of this Contract shall become or be an employee of the Contractor, as provided under MD Code, General Provisions § 5-501, *et seq*.

7. Non-employment of Contractor's employees

Nothing in this contract shall be construed to create an employment relationship between the AOC and any employee of either the Contractor or Contractor's subcontractors.

8. Disputes

Any claim regarding the proper interpretation of this Contract shall be submitted, in writing, to the Procurement Officer, together with a statement of grounds supporting the Contractor's interpretation. Pending resolution of a claim by the Procurement Officer, the Contractor shall proceed diligently with the performance of the Contract in accordance with the Procurement Officer's decision. An adverse decision to the Contractor may be appealed by the Contractor to the AOC within fifteen (15) days of the Procurement Officer's decision for adjudication pursuant to the Maryland Judiciary Procurement Policy.

9. Maryland Law

The place of performance of this Contract shall be the State of Maryland. This Contract shall be performed, construed, interpreted, and enforced according to the laws of the State of Maryland, including State Government Article § 12-204. No action relating to this contract shall be brought in any forum other than Maryland, whether or not the AOC is a party to such an action.

10. Non-discrimination in Employment

The Contractor agrees: (a) not to discriminate in any manner against any person because of race, color, religion, age, sex, marital status, national origin, physical or mental disability, familial status, genetic information, gender identity or expression, sexual orientation, or any other characteristic protected by State or federal law; (b) to include a provision similar to that contained in subsection (a), above, in any underlying subcontract; and (c) to post and to cause subcontractors to post in conspicuous places available to employees and applicants for employment, notices setting forth the substance of this clause.

11. Contingent Fee Prohibition

The Contractor warrants that it has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency working for the Contractor to solicit or secure this Contract, and that it has not paid or agreed to pay any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide salesperson, or commercial selling agency, any fee or other consideration contingent on the making of this Contract.

12. Non-availability of Funding

If the Maryland General Assembly fails to appropriate funds or if funds are not otherwise made available for continued performance for any fiscal year of this Contract succeeding the first fiscal year, this Contract shall be canceled automatically as of the beginning of the fiscal year for which funds were not appropriated or otherwise made available; provided, however, that this will not affect either the AOC's rights or the Contractor's rights under any termination clause in this Contract. The effect of termination of the Contract hereunder will be to discharge both the Contractor and the AOC from future performance of the Contract, but not from their rights and obligations existing at the time of termination. The Contractor shall be reimbursed for the reasonable value of any non-recurring costs incurred but not amortized in the price of the Contract. The AOC shall notify the Contractor as soon as it has knowledge that funds may not be available for the continuation of this Contract for each succeeding fiscal period beyond the first.

13. Termination for Cause

If Contractor fails to fulfill its obligations under this Contract properly and on time, or otherwise violates any provision of the Contract, the AOC may terminate the Contract by written notice to the Contractor. The notice shall specify the acts or omissions relied upon as cause for termination. All finished or unfinished work provided by the Contractor shall, at the AOC's option, become the AOC's property. The AOC shall pay the Contractor fair and equitable compensation for satisfactory performance prior to receipt of notice of termination, less the amount of damages caused by the Contractor's breach. If the damages are more than the compensation payable to the Contractor, the Contractor will remain liable after termination, and the AOC can affirmatively collect damages.

14. Termination for Convenience

The performance of work under this Contract may be terminated by the AOC in accordance with this clause in whole or, from time to time, in part whenever the AOC determines that such termination is in the AOC's best interest. The AOC will pay all reasonable costs associated with this Contract that the Contractor has incurred up to the date of termination, and all reasonable costs associated with termination of the Contract; however, the Contractor shall not be reimbursed for any anticipatory profits that have not been earned up to the date of termination.

15. Delays and Extensions of Time

The Contractor agrees to perform this Contract continuously and diligently. No charges or claims for damages shall be made by the Contractor for any delays or hindrances, regardless of cause, in the performance of services under this Contract. Time extensions may be granted only for excusable delays that arise from unforeseeable causes beyond the control and without the fault or negligence of the Contractor, including but not restricted to acts of God, acts of the public enemy, acts of the State in either its sovereign or contractual capacity, acts of another Contractor in the performance of an AOC contract, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, or the delay of a subcontractor or supplier arising from unforeseeable causes beyond the control and without the fault or negligence of either the Contractor or the subcontractor or supplier.

16. Suspension of Work

The AOC may direct the Contractor in writing to suspend, delay, or interrupt all or any part of its performance for such period of time as the Procurement Officer may determine to be appropriate for the AOC's convenience.

17. Pre-existing Law

The applicable statutes and regulations of the State of Maryland are hereby incorporated in this Contract.

18. Financial Disclosure

The Contractor shall comply with the provisions of § 13-221 of the State Finance and Procurement Article of the Annotated Code of Maryland.

19. Political Contribution Disclosure.

The Contractor shall comply with Title 14 of the Election Law of Maryland.

20. Right to Audit

20.1 The Contractor shall establish a reasonable accounting system, shall retain and maintain all records and supporting documents and materials relating to this Contract for five (5) years after final payment by the AOC hereunder and shall make them available for inspection and audit by authorized representatives of the State of Maryland and/or the AOC, including the Procurement Officer or the Procurement Officer's designee, at all reasonable times. The Contractor shall cooperate fully with any audits or investigations conducted by the State of Maryland and/or the AOC.

20.2 The AOC reserves the right, at its sole discretion at any time, to perform an audit of the Contractor's performance under this Contract. Auditing is defined as an independent objective assurance and consulting activity performed by qualified personnel including, but not limited to, the AOC's Internal Audit Department, to determine by investigation, examination, or evaluation of objective evidence from data, statements, records, operations, and performance practices (financial or otherwise), the Contractor's compliance with the Contract, including but not limited to adequacy and compliance with established procedures and internal controls over the Contract services being performed for the AOC.

20.3 Upon three (3) business days' notice, the Contractor shall provide the AOC reasonable access to their respective records to verify compliance with the terms of the Contract. The AOC may conduct these audits with any or all of its own internal resources or by securing the services of a third party accounting or audit firm, solely at the AOC's election. The AOC may copy, at its own expense, any record related to the services performed and provided under this Contract.

20.4 The right to audit shall include the Contractor's subcontractors including, but not limited to, any lower tier subcontractor(s) that provide essential support to the Contract services. The Contractor and/or subcontractor(s) shall ensure the AOC has the right to audit such subcontractor(s).

21. Liability for Loss of Data

In the event of loss of any data or records necessary for the performance of this Contract, which such loss is due to the error, negligence, or intentional act or omission of the Contractor, the Contractor shall be responsible, irrespective of cost to the Contractor, for recreating all such lost data or records in a manner, format, and time-frame acceptable to the AOC.

22. Subcontracting and Assignment

The Contractor may subcontract any portion of the services provided under this Contract by obtaining the Procurement Officer's prior written approval. The Contractor may assign this Contract, or any of its rights or obligations hereunder, only with the Procurement Officer's prior written approval. Any such subcontract or assignment shall be subject to any terms and conditions that the Procurement Officer deems necessary to protect the interest of the State of Maryland. The AOC shall not be responsible for the fulfillment of the Contractor's obligations to subcontractors.

23. Indemnification

23.1. The Contractor shall hold harmless and indemnify the AOC from and against any and all losses, damages, claims, suits, actions, liabilities, and/or expenses, including, without limitation, attorneys' fees and costs and disbursements of any character that arise from, are in connection with or are attributable to the performance or nonperformance of the Contractor or its subcontractors under this contract.

23.2 The AOC has no obligation to provide legal counsel or defense to the Contractor or its subcontractors in the event that a suit, claim or action of any character is brought by any person not party to this Contract against the Contractor or its subcontractors as a result of or relating to the Contractor's obligations under this Contract.

23.3 The AOC has no obligation for the payment of any judgments or the settlement of any claims against the Contractor or its subcontractors as a result of or relating to the Contractor's obligations under this Contract.

23.4 The Contractor shall immediately notify the Procurement Officer of any claim, suit or action made or filed against the Contractor or its subcontractors regarding any matter resulting from or relating to the Contractor's obligations under the Contract, and shall cooperate, assist and consult with the AOC in the defense or investigation of any such claim, suit, or action.

24. Limitation of Liability

Without prejudice to the AOC's right to pursue non-monetary remedies, Contractor shall be liable as follows:

24.1 For infringement of patents, trademarks, trade secrets, and copyrights, as provided in § 5 of this Contract;

24.2 For damages arising out of death or bodily injury or property damage, no limitation; and

24.3 For all other claims, damages, loss, costs, expenses, suits or actions in any way related to this Contract, regardless of the form of such actions, the Contractor's liability shall not exceed five (5) times the NTE amount. Notwithstanding the foregoing, the Contractor's liability for third-party claims shall be unlimited.

25. Public Information Act Notice

The AOC provides public access to records in accordance with § 4-101 *et seq.* of the General Provisions Article, Annotated Code of Maryland, and the Maryland Rules of Procedure, Rules 16-901 through 16-912. If a request is made to review any records pertaining to this contract, the Contractor may be contacted by the AOC, as circumstances allow, to express its views on the availability of requested information. The final decision on release of any information rests with the AOC.

26. Conflict of Interest

26.1 "Conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the State or the AOC, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage. "Conflict of interest" includes pending litigation in the Maryland courts.

26.2 "Person" includes a contractor, consultant, or subcontractor or sub consultant at any tier, and also includes an employee or agent of any of them if the employee or agent has or will have the authority to control or supervise all or a portion of the work for which a bid or offer is made.

26.3 The Contractor warrants that, except as disclosed in Section 26.4 below, there are no relevant facts or circumstances now giving rise or which could, in the future, give rise to a conflict of interest.

26.4 The following facts or circumstances give rise or could in the future give rise to a conflict of interest (Contractor: explain details-attach additional sheets if necessary; **if none, so state:**

_____

_____

26.5 The Contractor agrees that if an actual or potential conflict of interest arises after the contract commences, the Contractor shall immediately make a full disclosure in writing to the Procurement Officer of all relevant facts and circumstances. This disclosure shall include

a description of actions which the Contractor has taken and proposes to take to avoid, mitigate, or neutralize the actual or potential conflict of interest. If the contract has been awarded and performance of the contract has begun, the contractor shall continue performance until notified by the Procurement Officer of any contrary action to be taken. The existence of a conflict of interest is cause for termination of the Contract as well as disciplinary action against an employee for whom a conflict exists.

27. Ownership and Rights in Data

27.1 In addition to the requirements stated in the RFP, the Contractor agrees to furnish the AOC with copies of the following: computations, computer files, data, model(s), transmittal letters, response letters, training materials, and all other documents or correspondence pertinent to the operation of [insert type of Goods or Services].

27.2 The AOC shall be the owner of all materials developed under this Contract and shall be entitled to use, transfer, disclose, and copy them in any manner, without restriction and without compensation to the Contractor. Without AOC's prior written consent, the Contractor may neither use, execute, reproduce, display, perform, distribute (internally or externally), retain copies of, or prepare derivative works based on, these Materials nor authorize others to perform those acts.

27.3 The Contractor agrees that, at all times during the terms of this Contract and thereafter, all materials developed under this Contract, shall be "works for hire" as that term is interpreted under U.S. copyright law. To the extent that any of these materials are not works for hire for the AOC, the Contractor hereby relinquishes, transfers, and assigns to the AOC all of its rights, title, and interest (including all intellectual property rights) in such materials, and shall cooperate with the AOC in effectuating and registering any necessary assignments.

27.4 The AOC shall retain full ownership over any materials that the AOC provides to the Contractor under this Contract.

28. Notices

All notices required to be given by one party to the other hereunder shall be in writing and shall be addressed as follows:

State: **Khrystine Bunche**
Administrative Office of the Courts
2003 C Commerce Park Drive
Annapolis, MD 21401

Contractor: **(Company Name and Address)**

SIGNATURES:

Contractor:
(Company Name)

_____ (SEAL) Date: _____
Signature
Authorized Representative

For the Administrative Office of the Courts:

_____ Date: _____
Gisela K. Blades, Director
Procurement, Contract & Grant Administration

_____ Date: _____
Pamela Harris
State Court Administrator

_____ Date: _____
Mary Ellen Barbera
Chief Judge, Court of Appeals of Maryland

Approved for form and legal sufficiency this _____ day of _____, YEAR

_____
Stephane J. Latour
Managing Legal Counsel

ATTACHMENT B – BID PROPOSAL AFFIDAVIT (Authorized Representative and Affiant)

A. AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:
I am the (title) _____ and the duly authorized representative of (business) _____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

B. AFFIRMATION REGARDING BRIBERY CONVICTIONS
I FURTHER AFFIRM THAT:
Neither I, nor to the best of my knowledge, information, and belief, the above business (as is defined in Section 16-101(b) of the State Finance and Procurement Article of the Annotated Code of Maryland), or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities, including obtaining or performing Contracts with public bodies, has been convicted of, or has had probation before judgment imposed pursuant to Criminal Procedure Article, §6-220, Annotated Code of Maryland, or has pleaded nolo contendere to a charge of, bribery, attempted bribery, or conspiracy to bribe in violation of Maryland law, or of the law of any other state or federal law, except as follows (indicate the reasons why the affirmation cannot be given and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of person(s) involved, and their current positions and responsibilities with the business): **if none, so state:**

_____

_____

_____

C. AFFIRMATION REGARDING OTHER CONVICTIONS
I FURTHER AFFIRM THAT:
Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities including obtaining or performing contracts with public bodies, has:
(1) Been convicted under state or federal statute of:

(a) a criminal offense incident to obtaining, attempting to obtain, or performing a public or private contract; or

(b) fraud, embezzlement, theft, forgery, falsification or destruction of records, or receiving stolen property;

(2) Been convicted of any criminal violation of a state or federal antitrust statute;
(3) Been convicted under the provisions of Title 18 of the United States Code for violation of the Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. §1961, et seq., or the Mail Fraud Act, 18 U.S.C. §1341, et seq., for acts in connection with the submission of bids or proposals for a public or private contract;
(4) Been convicted of a violation of the State Minority Business Enterprise Law, Section 14-308 of the State Finance and Procurement Article of the Annotated Code of Maryland;

(5) Been convicted of a violation of the Section 11-205.1 of the State Finance and Procurement Article of the Annotated Code of Maryland;
(6) Been convicted of conspiracy to commit any act or omission that would constitute grounds for conviction or liability under any law or statute described in subsection (1) through (5) above;
(7) Been found civilly liable under a state or federal antitrust statute for acts or omissions in connection with the submission of bids or proposals for a public or private contract;
(8) Been found in a final adjudicated decision to have violated the Commercial Nondiscrimination Policy under Title 19 of the State Finance and Procurement Article of the Annotated Code of Maryland with regard to a public or private contract; or
(9) Admitted in writing or under oath, during the course of an official investigation or other proceedings, acts or omissions that would constitute grounds for conviction or liability under any law or statute described in Section B and subsections (1) through (7) above, except as follows (indicate reasons why the affirmations cannot be given, and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of the person(s) involved and their current positions and responsibilities with the business, and the status of any debarment): **if none, so state:**

_____

_____

_____

D. AFFIRMATION REGARDING DEBARMENT
I FURTHER AFFIRM THAT:
Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities, including obtaining or performing contracts with public bodies, has ever been suspended or debarred (including being issued a limited denial of participation) by any public entity, except as follows (list each debarment or suspension providing the dates of the suspension or debarment, the name of the public entity and the status of the proceedings, the name(s) of the person(s) involved and their current positions and responsibilities with the business, the grounds of the debarment or suspension, and the details of each person's involvement in any activity that formed the grounds of the debarment or suspension): **if none, so state:**

_____

_____

_____

E. AFFIRMATION REGARDING DEBARMENT OF RELATED ENTITIES
I FURTHER AFFIRM THAT:
(1) The business was not established and it does not operate in a manner designed to evade the application of or defeat the purpose of debarment pursuant to Sections 16-101, et seq., of the State Finance and Procurement Article of the Annotated Code of Maryland; and
(2) The business is not a successor, assignee, subsidiary, or affiliate of a suspended or debarred business, except as follows (you must indicate the reasons why the affirmations cannot be given without qualification): **if none, so state:**

_____

_____

_____

F. SUB-CONTRACT AFFIRMATION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, has knowingly entered into a contract with a public body under which a person debarred or suspended under Title 16 of the State Finance and Procurement Article of the Annotated Code of Maryland will provide, directly or indirectly, supplies, services, architectural services, construction related services, leases of real property, or construction.

G. AFFIRMATION REGARDING COLLUSION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business has:

(1) Agreed, conspired, connived, or colluded to produce a deceptive show of competition in the compilation of the accompanying bid or offer that is being submitted;

(2) In any manner, directly or indirectly, entered into any agreement of any kind to fix the bid price or price proposal of the bidder or Offerors or of any competitor, or otherwise taken any action in restraint of free competitive bidding in connection with the contract for which the accompanying bid or offer is submitted.

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, Election Law Article, §§14-101—14-108, Annotated Code of Maryland, which requires that every person that enters into contracts, leases, or other agreements with the State of Maryland, including its agencies or a political subdivision of the State, during a calendar year in which the person receives in the aggregate $100,000 or more shall file with the State Board of Elections a statement disclosing contributions in excess of $500 made during the reporting period to a candidate for elective office in any primary or general election.

H. CERTIFICATION OF CORPORATION REGISTRATION AND TAX PAYMENT

I FURTHER AFFIRM THAT:

(1) The business named above is a (domestic ___) (foreign __) corporation registered in accordance with the Corporations and Associations Article, Annotated Code of Maryland, and that it is in good standing and has filed all of its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation, and that the name and address of its resident agent filed with the State Department of Assessments and Taxation is (IF NOT APPLICABLE, SO STATE): **if none, so state:**

Name: _____

Address: _____

_____

_____

(2) Except as validly contested, the business has paid, or has arranged for payment of, all taxes due the State of Maryland and has filed all required returns and reports with the Comptroller of the Treasury, the State Department of Assessments and Taxation, and the Department of Labor, Licensing, and Regulation, as applicable, and will have paid all withholding taxes due the State of Maryland prior to final settlement.

I. CONTINGENT FEES

I FURTHER AFFIRM THAT:

The business has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency working for the business, to solicit or secure the Contract, and that the business has not paid or agreed to pay any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency, any fee or any other consideration contingent on the making of the Contract.

J. ACKNOWLEDGEMENT

I ACKNOWLEDGE THAT this Affidavit is to be furnished to the Procurement Officer and may be distributed to units of: (1) the State of Maryland; (2) counties or other subdivisions of the State of Maryland; (3) other states; and (4) the federal government. I further acknowledge that this Affidavit is subject to applicable laws of the United States and the State of Maryland, both criminal and civil, and that nothing in this Affidavit or any contract resulting from the submission of this bid or proposal shall be construed to supersede, amend, modify or waive, on behalf of the State of Maryland, or any unit of the State of Maryland having jurisdiction, the exercise of any statutory right or remedy conferred by the Constitution and the laws of Maryland with respect to any misrepresentation made or any violation of the obligations, terms and covenants undertaken by the above business with respect to (1) this Affidavit, (2) the contract, and (3) other Affidavits comprising part of the contract.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By: _____
(Authorized Representative and Affiant)

ATTACHMENT C – CONTRACT AFFIDAVIT

CONTRACT AFFIDAVIT

A. AUTHORITY

I HEREBY AFFIRM THAT:

I, _____ (print name), possess the legal authority to make this Affidavit.

B. CERTIFICATION OF REGISTRATION OR QUALIFICATION WITH THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION

I FURTHER AFFIRM THAT: _____

The business named above is a (check applicable box):

(1) Corporation — ☐ domestic or ☐ foreign;
(2) Limited Liability Company — ☐ domestic or ☐ foreign;
(3) Partnership — ☐ domestic or ☐ foreign;
(4) Statutory Trust — ☐ domestic or ☐ foreign;
(5) ☐ Sole Proprietorship.

and is registered or qualified as required under Maryland Law. I further affirm that the above business is in good standing both in Maryland and (IF APPLICABLE) in the jurisdiction where it is presently organized, and has filed all of its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation. The name and address of its resident agent (IF APPLICABLE) filed with the State Department of Assessments and Taxation is: **if none, so state):**

Name: _____
Department ID Number: _____
Address:_____

and that if it does business under a trade name, it has filed a certificate with the State Department of Assessments and Taxation that correctly identifies that true name and address of the principal or owner as: **if none, so state):**

Name: _____
Department ID Number: _____
Address:_____

C. POLITICAL CONTRIBUTION DISCLOSURE AFFIRMATION

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, Election Law Article, §§14-101 — 14-108, Annotated Code of Maryland, which requires that every person that enters into contracts, leases, or other agreements with the State of Maryland, including its agencies or a political subdivision of the State, during a calendar year in which the person receives in the aggregate $100,000 or more shall file with the State Board of Elections a statement disclosing contributions in excess of $500 made during the reporting period to a candidate for elective office in any primary or general election.

D. CERTAIN AFFIRMATIONS VALID

I FURTHER AFFIRM THAT:

To the best of my knowledge, information, and belief, each of the affirmations, certifications, or acknowledgements contained in that certain Bid/Proposal Affidavit dated _____ , 20___ , and executed by me for the purpose of obtaining the contract to which this Exhibit is attached remains true and correct in all respects as if made as of the date of this Contract Affidavit and as if fully set forth herein.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____

By: _____
(printed name of Authorized Representative and Affiant)

_____
(signature of Authorized Representative and Affiant)

ATTACHMENT D – PRE-PROPOSAL CONFERENCE RESPONSE FORM

Project No. K18-0036-29

Project Title: Emergency Mass and IT Alert Notification System

Pre-Proposal Conference: October 30, 2017

Please e-mail this form to the Procurement Officer:

Khrystine.Bunche@mdcourts.gov

By October 27, 2017 at noon advising whether or not you plan to attend this Conference.

Please indicate:

_____ Yes, the following representatives will be in attendance:

1.

2.

_____ No, we will not be in attendance.

_____ _____

Company/Firm/Company Name Telephone

_____

Contact Name

ATTACHMENT E – PRICE PROPOSAL FORM

EMERGENCY MASS AND IT ALERT NOTIFICATION SYSTEM

PRICE PROPOSAL FOR RFP # K18-0036-29

	Price
Implementation Services (Base Year One)	$
Project Management Services (Base Year One)	$
Licensing (Base Year One) @75 users	$
Data Conversion (Base Year One)	$
Additional Modules • Detail the cost associated with any additional modules required to meet system requirements. List the Requirement Number for each additional module indicated. (Base Year One)	$
	$
	$
	$
	$
Major Customization • Detail the cost associated with any requirement which requires major customization. List the Requirement Number, the associated hourly cost(s) and the Requirement total cost. (Base Year One)	$
	$
	$
	$
	$
Total Price (Base Year One)	**$**
Implementation Services (Base Year Two)	$
Project Management Services (Base Year Two)	$
Licensing (Base Year Two) @75 users	$
Data Conversion (Base Year Two)	$
Additional Modules • Detail the cost associated with any additional modules required to meet system requirements. List the Requirement Number for each additional module indicated. (Base Year Two)	$
	$
	$
	$
	$
Major Customization • Detail the cost associated with any requirement which requires major customization. List the Requirement Number, the associated hourly cost(s) and the Requirement total cost. (Base Year Two)	$

	$
	$
	$
	$
Total Price (Base Year Two)	**$**
Implementation Services (Option Year One)	$
Project Management Services (Option Year One)	$
Licensing (Option Year One) @75 users	$
Data Conversion (Option Year One)	$
Additional Modules • Detail the cost associated with any additional modules required to meet system requirements. List the Requirement Number for each additional module indicated. (Option Year One)	$
	$
	$
	$
	$
Major Customization • Detail the cost associated with any requirement which requires major customization. List the Requirement Number, the associated hourly cost(s) and the Requirement total cost. (Option Year One)	$
	$
	$
	$
	$
Total Price (Option Year One)	**$**
Implementation Services (Option Year Two)	$
Project Management Services (Option Year Two)	$
Licensing (Option Year Two) @75 users	$
Data Conversion (Option Year Two)	$
Additional Modules • Detail the cost associated with any additional modules required to meet system requirements. List the Requirement Number for each additional module indicated. (Option Year Two)	$
	$
	$
	$
	$
Major Customization • Detail the cost associated with any requirement which requires major customization. List the Requirement Number, the associated hourly cost(s) and the Requirement total cost. (Option Year Two)	$
	$
	$
	$

	$
Total Price (Option Year Two)	**$**
Implementation Services (Option Year Three)	$
Project Management Services (Option Year Three)	$
Licensing (Option Year Three) @75 users	$
Data Conversion (Option Year Three)	$
Additional Modules • Detail the cost associated with any additional modules required to meet system requirements. List the Requirement Number for each additional module indicated. (Option Year Three)	$
	$
	$
	$
	$
Major Customization • Detail the cost associated with any requirement which requires major customization. List the Requirement Number, the associated hourly cost(s) and the Requirement total cost. (Option Year Three)	$
Total Price (Option Year Three)	$
	$
Total NTE	**$**

ATTACHMENT F – NON-DISCLOSURE AGREEMENT

THIS NON-DISCLOSURE AGREEMENT ("Agreement") is made as of this ___ day of _____, 2017, by and between Administrative Office of the Courts ("AOC") and _____ (Contractor"), a corporation with its principal business office located at _____ and its principal office in Maryland located at _____.

RECITALS

WHEREAS, the Contractor and AOC have entered into Contract No. **K18-0036-29**_____ (**the "Contract**); and

WHEREAS, in order for Contractor to perform the work required under the Contract, or in the course of that work, the Contractor, the Contractor's subcontractors, and the Contractor's and subcontractors' employees and agents (**collectively the "Contractor's Personnel"**) may come into contact with information maintained or held by the Judicial branch of the Maryland government ("Confidential Information"), including the AOC and all courts, units and departments **(collectively "the Judiciary")**; and

WHEREAS, the Judiciary, in order to comply with the law, fulfill its various missions, and enhance the safety of participants in the judicial process, must ensure the confidentiality of certain information, and, to that end, must act as the sole entity with the authority to determine which information held by the Judiciary may be disclosed to persons or entities outside of the Judiciary; and

WHEREAS, Contractor acknowledges that Contractor's compliance with this Agreement is a condition of doing business with AOC,

NOW, THEREFORE, Contractor agrees as follows:

1. "Confidential Information" includes any and all information provided by or made available by the Judiciary to Contractor's Personnel in connection with the Contract, regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such or disclosed deliberately or inadvertently. Such information is Confidential Information, whether or not its contents may also be gathered from other sources, or may subsequently be disseminated to the public. Confidential Information includes, by way of example only, information that the Contractor's Personnel sees, views, hears, takes notes from, copies, possesses or is otherwise provided access to and use of by the Judiciary, whether the information relates to the Contract or the Contract has placed the Contractor's Personnel in the position to receive the information. Confidential information further includes information both held by the Judiciary and derived or created from information held by the Judiciary.

2. Contractor's Personnel shall not, without the AOC's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information, except for the sole and exclusive purpose of performing under the Contract and except for disclosures to such Judiciary employees whose knowledge of the information is necessary to the performance of the Contract. Contractor shall limit access to the Confidential Information to Contractor's Personnel who: 1) have a demonstrable need to know such Confidential Information in order to perform Contractor's duties under the Contract and 2) have agreed with Contractor in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. The names of Contractor's Personnel are attached hereto and made a part hereof as Exhibit 1. With respect to information pertaining to the job performance, skills, or conduct of any Judiciary employee, the ***only*** **person with the need to know such information is _____**, and, except in cases of emergency involving imminent or actual bodily harm or significant property loss or damage, such information may only be disseminated to him, or, in his absence, to the State Court Administrator.

3. Contractor shall require each employee, agent, and subcontractor whose name appears on Exhibit 1 to sign a writing acknowledging receipt of a copy of , and agreeing to comply with the terms and conditions of, this Agreement. Subcontractors shall expressly agree to all of the terms applicable to Contractor. Accordingly, subcontractors must require

their employees and agents to sign such a writing and must submit those individuals' names to the Contractor for inclusion on Exhibit 1. Upon the Procurement Officer's request, Contractor shall provide originals of all such writings to the AOC. Contractor and subcontractors shall update Exhibit 1 by adding additional names as needed and shall ensure that no employee or agent comes into contact with Confidential Information before that person has signed this Agreement. This Agreement shall not be construed to create a employment relationship between AOC and any of Contractor's or subcontractors' personnel.

4. If Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in Contractor's performance of the Contract or who will otherwise have a role in performing any aspect of the Contract, Contractor shall first obtain AOC Contract Manager's written consent to any such dissemination. AOC's Contract Manager may grant, deny, or condition any such consent, as it may deem appropriate in the Contract Manager's sole and absolute subjective discretion.

5. Contractor shall hold the Confidential Information in trust and in strictest confidence, adopt or establish operating procedures and physical security measures, take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to, or theft by, unauthorized third parties, and prevent all or any portion of the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.

6. Contractor shall promptly advise the AOC Contract Manager in writing if Contractor learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of Contractor's Personnel or the Contractor's former Personnel. Contractor shall, at its own expense, cooperate with AOC in seeking damages and/or injunctive or other equitable relief against any such person(s).

7. Upon the earlier of AOC's request or termination of the Contract, Contractor shall, at its own expense, return to the Contract Manager , all copies of the Confidential Information, no matter how formatted or stored, in Contractor's and/or Contractor's Personnel's care, custody, control or possession.

8.A breach of this Agreement by the Contractor or noncompliance by Contractor's Personnel with the terms of this Agreement shall also constitute a breach of the Contract. The termination of the Contract does not terminate Contractor's obligations under this Agreement.

9. Contractor acknowledges that any failure by the Contractor or Contractor's Personnel to abide by the terms of this Agreement may cause irreparable harm to the Judiciary and that monetary damages may be inadequate to compensate the Judiciary for such breach. Accordingly, the Contractor agrees that the AOC may, in addition to any other remedy available to AOC under Maryland and any applicable federal law, seek injunctive relief and/or liquidated damages of $1,000 for each unauthorized disclosure. Contractor consents to personal jurisdiction in the Maryland State Courts and to the application of Maryland law, if AOC so elects in its sole discretion, irrespective of Maryland's conflict-of-law rules. If the Judiciary suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part, to any failure by the Contractor or any of the Contractor's Personnel to comply with the requirements of this Agreement, the Contractor shall hold harmless and indemnify the Judiciary from and against any such losses, damages, liabilities, expenses, and/or costs.

10. The parties further agree that 1) Contractor's rights and obligations under this Agreement may not be assigned or delegated, by operation of law or otherwise, without AOC's prior written consent; 2) the invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall be construed to provide the broadest possible protection against the disclosure of Judiciary information; 3) signatures exchanged by facsimile are effective for all purposes hereunder to the same extent as original signatures; and 4) the Recitals are not merely prefatory but are an integral part hereof.

Contractor: **Administrative Office of the Courts**

By:_____Date:_____ Received by: _____

Name:_____ Date:_____

[Exhibit 1 dated: _____]

ATTACHMENT G – SYSTEM REQUIREMENTS FORM

General Requirements

#	Description	Response
1.0	**General**	
1.1	Is your system offered as a SaaS solution (Software as a Service)?	
1.2	Describe the guaranteed Service Level and uptime for your hosted solution.	
1.3	Do you have secure redundant locations for your hosted solution as part of the standard service offering? If not, please describe redundant capabilities.	
1.4	Do you offer multiple environments for the solution (i.e., prod, dev, and test) at no additional cost? If not, please describe your non-prod offerings and any associated costs, one-time or ongoing.	
1.5	Do you provide 24x7 technical support for the solution at no additional cost? If not, please describe your technical support model and associated costs.	
1.6	Do you provide unlimited messaging for email, SMS, and Voice? If not, please describe your cost model.	
1.7	Is the User interface available in multiple languages. If so, for which ones?	
1.8	Is the user interface web-based? Is it simple to understand and use, especially for non-IT users? Does the system support the ability to create and modify notification forms from the web interface? Does your system have a drag-and-drop user interface for easy customization of fields? Does your system have message templates? Does your system have the ability to change any field, field value, or field type on a message template?	
1.9	Describe your solution's message delivery channels. Please address: • Phone • Text messages (SMS) • Fax • Pager • Email • Mobile App push messages • Instant Messages • Social Media	
1.10	Does your system have the ability to deliver two-way communications on all communication channels listed previously to facilitate acknowledgment?	

1.11	Will your system lag when there is a large volume of messages to send out or receive? What is the published throughput of your system?	
1.12	Does your system provide the ability to cancel/clear messages in a queue waiting to be delivered?	
1.13	Does your system have any tool to migrate data from Rave?	
1.14	How are regular system backups accomplished?	
1.15	Do you support alternative push channels if there is a system crash or overload? If so, please describe.	

Security Requirements Overview

#	Description	Response
2.0	**Security**	
2.1	Describe the authentication process employed for your solution including any web-based integration techniques for user authentication.	
2.2	Does the system support Single Sign On?	
2.3	Does the system offer role-based security management to protect sensitive information? Can security profiles for users be easily configured through the user interface?	
2.4	Are there any limits on the type and number of Roles available?	
2.5	Does your solution offer an unlimited number of administrative roles with varying degrees of security rights?	
2.6	Can your system use Active Directory groups at our premise for role-based authorization?	
2.7	If authenticating directly with your solution vs. Active Directory what encryption mechanism is used to store the password?	

Integration Requirements

#	Name	Answer
3.0	**Integration**	
3.1	Is there a REST or SOAP (Web Services) API included with the product at no additional charge? Does your system have programmatic triggering of activation from other applications?	
3.2	Does the system have business rules to escalate incident ticket and monitoring alert based on their status, priority and alert type?	
3.3	Do you interface with ServiceNow? If so, how?	

Data Management Requirements

#	Name	Answer
4.0	**Data Management**	
4.1	Can the system synchronize user data from existing sources such as Active Directory, LDAP, corporate PeopleSoft HCM, ServiceNow and others? If yes, please describe.	
4.2	Can the system synchronize user data from multiple sources?	
4.3	Does the solution have the ability to import and/or update contact information from .csv or Excel?	
4.4	Does the solution have the ability to export contact information to Excel or .csv?	
4.5	Can the user data model be extendable to support the tracking of skills, certifications and other user defined attributes (expertise/coverage area, job title, etc.)?	
4.6	Is there a limit on the number of devices the system can send messages to for an individual user?	
4.7	Does the system provide a way to test and validate devices (i.e., SMS, email, voice, etc.)?	
4.8	Does your solution have the ability to add and edit contact information directly within the system?	
4.9	Does your system allow users to specify when they want to be notified on individual devices?	

4.10	Are users able to update their own personal contact information without having access to another person's data?	
4.11	Can Recipients specify the order of contact devices they can receive a message (e.g. cell phone 1, and if no response, cell phone 2, and if no response, email, and if no response, home phone, etc.).	
4.12	Does your system allow users to subscribe to certain notifications based on alert criteria/business rule?	

Group and Escalation Requirements

#	Name	Answer
5.0	**On Call Group & Escalation Management**	
5.1	Does the system support defining permissions and roles to limit who has the ability to create and modify on-call groups/schedules? Can this authorization be controlled using on-premise Active Directory groups? If not, describe how these functions are accomplished within your system.	
5.2	Does the system support defining complex on-call schedules based on multiple shifts, coverage times, rotation patterns and escalation order?	
5.3	Can the conference call initiator view who is on call at any given time?	
5.4	Does your solution have the ability to create and track groupings of recipients by team, department, location, etc.?	
5.5	Does your system have the ability to assign recipients to groups based on active directory groups, directory attributes, contact data, GIS mapping, and ServiceNow information? Please elaborate.	
5.6	Does your solution have the ability to create hierarchical groupings to reflect an organization’s structure?	
5.7	Can a recipient be a member of any number of groups or teams?	
5.8	Does the system support the defining of Holiday Schedules & coverages?	
5.9	Does the system support the ability for the individual to define temporary replacements when they go on vacation, PTO, etc.?	

Notification Requirements

#	Name	Answer
6.0	Notifications	
6.1	Does your system allow customers to create notification templates without vendor assistance?	
6.2	Does your system allow customizing fields and field values without vendor assistance and consulting services?	
6.3	Can the customized fields be prepopulated with data from various customer systems, such as ServiceNow?	
6.4	Can one customized field selection limit the list of options presented in another customized field?	
6.5	Does your system allow associating templates with distribution lists?	
6.6	Does your system have a drag-and-drop user interface that dynamically updates your smartphone application?	
6.7	Which methods can activate messages through your system? • Touchtone • IVR • Email • Web (list which browsers) • Smartphone App • Smartphone browsers • Vendor operator-assisted	
6.8	Does your system have the ability to deliver text-to-speech messages?	
6.9	Is your system able to send notifications to multiple devices for a user simultaneously?	
6.10	Is your system able to dynamically deliver different message formats (sms, email, voice) to different devices?	
6.11	Does the system support notification in multiple languages? If so, which languages are supported?	
6.12	Is your system able to escalate through multiple devices based on non-response?	
6.13	Does your system message a user only once in the case that they are a member of multiple groups?	
6.14	Can reusable/standard messages be created to be selected from a list when needed?	
6.15	Can your system customize the sender ID for the following communication channels: • Voice • Email • SMS • Fax	
6.16	Does your system have the ability to deliver pre-recorded voice notifications/messages?	
6.17	Does your system support file attachments to accompany messages/notifications?	

6.18	Does the system allow the sender to prioritize the notifications being sent?	
6.19	Can the sender override the recipient's device priority?	
6.20	Can the sender notify a user without seeing her/his contact information?	
6.21	Can the sender send to a group of recipients by sending to a group name only?	
6.22	Can a sender send a notification based on a selected area on a map? If yes, how do the recipients/groups within the map get populated?	
6.23	Does the sytem provide Autofill capabilities when typing in a name of recipients or groups?	
6.24	Do automated notifications escalate through the escalation path specified in the group if an acknowledgement has not been received in a specified amount of time? If not, describe the escalation process.	
6.25	Can notifications be targeted to users based on ad-hoc definitions of user attributes such as skill, certifications and other attributes (e.g., building, location, job title, etc.)?	
6.26	Does your system provide the ability to instantly route people to a conference bridge? If so, is it built into the messaging process so users are automatically put onto a bridge? If not, please describe your process for conference bridging.	
6.27	Does your system have complete dashboard and reporting for conference call management? If yes, please describe your capabilities.	
6.28	Does your system allow for devices that permit two-way notifications for the recipient of message to respond back to the sender (e.g., two way SMS, voice callback on key pad, etc.)?	
6.29	Can the recipient read or listen to the notification/message after the message has reached a set expiration time?	
6.30	Does your system support opt in/opt out for end users by message type?	
6.31	Can the system support "FYI" alerting and provide subscription services? Can a user be provided the ability to sign up to receive notifications based on user defined criteria or categories of messages? Please elaborate.	
6.32	Can your system send an update to a previously sent notification?	
6.33	Can your system be used to send periodic reminder notifications at a defined interval based on notification template and business rule? Does the system provide a dashboard/report on when the next notifications will be sent?	
6.34	What is the maximum number of messages that can be sent in a single event?	
6.35	Does the system allow secure communication between groups? Manager to all payroll staff? Manager to all security personnel? Message to all essential personnel in a court?	
6.36	Does the system provide for a review of a message before it is released for distribution?	
6.37	Does the system retry failed notifications? If yes, how many times or is this configurable?	

Reporting Requirements

#	Name	Answer
7.0	Reporting	
7.1	User can view the status of notifications in real-time for at least 24 hours of activity. Information to include who sent it, when it was sent, number of attempts, acknowledgement status, and the message content.	
7.2	Provide historical information of who sent a message, when it was sent, number of attempts, acknowledgement status, and the message sent.	
7.3	User can extract data to develop their own reports (e.g., metrics). What export formats do you support?	
7.4	Does your solution have logging capability? What is logged? What is the logging retention? Can logs be targeted to a centralized third party logging tool? Can access to the logs be limited by role?	
7.5	Does your solution log every message sent including: • Message content • Recipients • Responses • Carrier/aggregator information	
7.6	Does your system log every change to contact information?	
7.7	Does your system provide a tracking report to show real-time status for delivery and response? Does your system notify/report on failed deliveries? Does the system provide real time reports displaying the success / failure / responses of the messages sent with drill down capabilities to see additional details? Are you able to view real time reports on success /failure/ responses for the message sent from a smartphone?	
7.8	Does your system provide a report card to track delivery and response service levels or objectives?	
7.9	Does your system provide real-time views for conference bridge attendees?	
7.10	Does your system provide reports on user and call tree or group performance?	

Mobility Requirements

#	Name	Answer
8.0	Mobility	
8.1	Do you provide a mobile application? If so, which OS are supported? (iOS and Android?)	
8.2	Can you send a notification from your mobile app?	
8.3	Is registration required for the mobile app? If so, please describe the process.	
8.4	Does the mobile app provide recipient contact searching and display her/his contact information?	

Implementation, Training and Support

Requirement	Response
Describe any tools or services provided to maximize service adoption and registrations. Any additional costs should be clearly detailed in the pricing section below.	
Proposer's solution shall include initial training for system administrators and operators. Describe proposed training and detail any additional cost for future training.	
Provide a brief description of the major steps in the implementation process, including client resource needs, any on-premise activities required and timelines.	
Proposer must provide 24/7/365 phone support. Describe the support levels.	
Describe the support process provided.	
Describe any ongoing resource requirements expected from the institution.	
Proposer should provide an advanced training learning management environment that is available 24 hours a day. Describe offerings and usage.	
Access to training resources should be unlimited.	
Training resources should be supported on personal computers and via a mobile application supporting at least iOS and Android mobile devices. Describe functionality.	
Proposer's training system should offer a certification process that validates successful completion of courseware.	

Administrative Office of the Courts

Judicial Information Systems

Information Security Policy

March 2017

Table of Contents

PURPOSE

The purpose of this Policy is to describe the security guidelines that the Maryland Judiciary must consider when protecting the confidentiality, integrity and availability of Judiciary owned information. This Policy establishes the general requirements and responsibilities for protecting Judiciary systems and information. All individuals utilizing Judiciary assets must comply with the security controls established in this Policy.

SCOPE

This Policy applies to anyone provided access to Judiciary technology assets including but not limited to information that is generated, received, stored, transmitted or printed.

The policy encompasses:

- All courts, units and departments of the Judicial Branch of the State of Maryland that access the Judicial Information Systems (JIS) network.
- All activities and operations required to ensure data security. This includes facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights.

AUTHORITY

The Chief Judge of the Court of Appeals is the establishing authority for this Policy with the advice and guidance of the Judicial Council.

The Chief Judge of the Court of Appeals or the State Court Administrator has the authority to exempt a category of users from any requirement of this Policy.

SECTION 1: Preface

Information and information technology (IT) systems are essential assets of the Maryland Judiciary and vital resources to Maryland citizens. These assets are critical to the services that the Judiciary provides to citizens and local and federal government entities. All information created with Judiciary resources for Judiciary operations is the property of the Maryland Judiciary. All users of the Judiciary's IT assets, including contractors and other third parties, are responsible for protecting those assets from unauthorized access, modification, disclosure, damage and destruction. This Policy sets forth a minimum level of security controls that, when implemented, will provide for the confidentiality, integrity and availability of Judiciary IT assets.

In general, the Judiciary will adopt information security leading practice standards and guidelines. This Policy developed to secure the Judiciary's IT assets will, where appropriate, refer to a particular standard. Judiciary security procedures will be documented to ensure compliance with the Policy. The Policy will be reviewed on an annual basis.

SECTION 2: Roles and Responsibilities

This Policy sets the minimum level of responsibility for the following individuals and/or groups:

- Administrative Office of the Courts (AOC)
- Court Technology Committee of the Judicial Council (CTechCom)
- JIS Assistant Administrator
- JIS Information Security Senior Manager
- Users of Judiciary Assets

2.1 Administrative Office of the Courts (AOC) CTechCom

The Judicial Council will serve as the governing body to oversee this Policy. CTechCom will be responsible for reviewing this Policy annually and for reporting findings and recommendations to the Judicial Council at least annually. The AOC will provide guidance and recommendations regarding IT security to CtechCom.

2.2 JIS Assistant Administrator

The JIS Assistant Administrator shall:

- Ensure that security is considered and integrated into all Judiciary information technology plans and objectives.
- Serve as the Liaison for JIS on the CTechCom.

2.3 JIS Information Security Senior Manager

The JIS Information Security Senior Manager shall:

- Review and update this Policy annually.
- Develop, implement and continue to mature the Security Program.
- Present changes and updates to this Policy and the Security Program to the CTechCom by April 1st.

- Employ the appropriate measures to assure and demonstrate compliance with this Policy.
- Ensure the JIS business continuity of operations (COOP) and disaster recovery (DR) plans for critical JIS systems are reviewed, updated and exercised (tested) annually.
- Conduct regular external and internal vulnerability assessments to verify security controls are working properly and to identify risks.
- Assure the confidentiality, integrity, availability, and accountability of all Judiciary electronic information assets while it is being used, processed, stored, or transmitted, and the security of the resources associated with those processing functions.
- Develop, implement and maintain an incident management process.
- Assume the lead role in resolving Judiciary security and privacy incidents.
- Lead efforts to formally educate Judiciary users on safe security practices.

2.4 Users of Judiciary Assets

All users of the Judiciary's IT assets are responsible to:

- Be aware of and comply with this Policy and associated standards, procedures and guidelines.
- Understand her/his responsibilities for protecting IT assets of the Judiciary.
- Use IT assets and resources only for authorized business purposes as defined by policies, laws and regulations of the Judiciary or the State.
- Be accountable for her/his actions relating to her/his use of all JIS managed IT systems and information.
- Be responsible for her/his assigned account. Users are prohibited from sharing her/his account credentials with others, including with other Judiciary personnel, except as otherwise provided by Policy.
- Understand that violation of security policy is subject to disciplinary action, where applicable or set by Rule.

SECTION 3: Asset Management

An inventory of all critical IT assets is required as directed by the JIS Assistant Administrator. Accountability for assets helps to ensure that appropriate protection is maintained. Designated owners shall be identified (Data Owners and Custodians) for all critical assets and assigned responsibility for the maintenance of appropriate controls.

3.1 Inventory of Assets

Compiling an inventory of assets is an important aspect of risk management. JIS needs to be able to identify Judiciary IT assets and the relative values and importance of these assets.
Based on this information, JIS can then provide appropriate levels of protection. Inventories of the critical assets associated with each information system should be documented and maintained. Asset inventories shall include, at a minimum; a unique system name, a designated owner and a description of the physical location of the asset. Examples of assets associated with information systems are:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster recovery plans, archived information.
- Software assets: application software, system software, development tools and utilities.

- Physical assets: computer equipment (processors, monitors, laptops, portable devices such as a flash/thumb drive, tablets, smartphones, etc.), communication equipment (routers, PBXs, fax machines, printers, etc.), magnetic/digital media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units).
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

3.2 Data Classification Policy

This Policy pertains to all information within the Judiciary's IT systems that is processed, stored, transmitted or shared. Data Owners and Custodians must adhere to this Policy and educate users who may have access to confidential information for which they are responsible.

All Judiciary IT information is categorized into two main classifications with regard to disclosure and protection:

- Public
- Confidential

Public information is information that has been declared publicly available by law or Rule. Public records are any records that are made or received by a covered public agency in connection with the transaction of public business.

Confidential information is non-public information that is defined by law or Rule that must be withheld from public access. This may include, but is not limited to, Personally Identifiable Information (PII), sealed information and Parties Only information.

Personally Identifiable Information (PII): Personally Identifiable Information is defined as an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with any one of the following:

- Social Security Number
- A Driver's License Number, State Identification Card Number, or other individual identification issued by a state agency
- A passport Number or other identification number issued by the United States Government
- An individual Taxpayer Identification Number
- A Financial or other account number, a credit card number, or debit card number that, in combination with any required security code, access code, or password would permit access to an individual's account.
- Any information that is defined as PII by statute or rule.

If a user is uncertain of the classification of a particular piece of information, the user should contact their manager for clarification.

To the extent required by Rule, all confidential information should be clearly identified as such and will be subject to marking and handling guidelines.

3.1 Guidelines for Marking and Handling Confidential Judiciary Information

To the extent required by Rule, Judiciary confidential information shall be protected and marked in accordance with the data sensitivity. Users shall not electronically store data that cannot be adequately secured against unauthorized access.

3.2 Security Categorization Applied to Information Systems

JIS will classify systems consistent with the classification of the data within the system. When an IT System is shared between the Judiciary and external parties, the most sensitive level of data classification will determine the classification of the IT System.

SECTION 4: Security Controls Overview

This section defines requirements that must be met by the Judiciary to properly protect judiciary assets. All Judiciary IT assets (hosted on the Judiciary network or a 3rd party offsite premise) used for receiving, processing, storing and transmitting Judiciary data must be protected in accordance with these controls. Information systems include the equipment, facilities, and people that handle or process Judiciary data.

These security controls are categorized into three types:

- Managerial
- Operational
- Technical

Managerial security controls focus on managing organizational risk and information system security and devising sufficient countermeasures for mitigating risk to acceptable levels.
Managerial security controls include, but are not limited to, risk management and project management.

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or a group of systems. Operational security controls require technical or specialized expertise and often rely on managerial and technical controls. Operational security controls include awareness and education, configuration management, service interface agreements, contingency planning, incident response, maintenance, media protection, physical and personnel security, system and information integrity, and system development life cycle methodology (SDLC).

Technical security controls focus on operations executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security controls include access control, audit and accountability, authentication and authorization, user authentication and password requirements, and system and communications.

SECTION 5: Managerial Level Controls

5.1 Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for the Judiciary to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess the acceptable risk to Judiciary IT systems.

As part of a risk-based approach used to determine adequate security for its IT assets, the Judiciary shall implement a process to assess the acceptable risk to Judiciary IT assets. The Judiciary shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.

5.2 Project Planning

Judiciary Information Technology projects, including system development, enhancement, maintenance, and infrastructure activities shall be managed to ensure that delivered solutions are consistent with this Policy.

Plans for executing IT projects should include a general process for addressing IT security controls. JIS shall ensure that all major IT development or infrastructure projects have a corresponding project plan that addresses the security control requirements within this Policy. JIS Information Security shall be an integral part of this planning process.

SECTION 6: Operational Level Controls

6.1 Awareness and Education

The Judiciary must ensure all information system users and managers are knowledgeable of security awareness and are provided educational material before authorizing access to systems. JIS must identify personnel with information system security roles and responsibilities, document those roles and responsibilities, and provide sufficient security training before authorizing access to information systems or confidential information. JIS must document and monitor individual information system security training activities including basic security education and awareness training and specific information system security training.

6.2 Configuration Management

System hardening procedures shall be created and maintained to ensure up-to-date security leading practices are deployed for all IT operating systems, applications, databases and network devices. All default system administrator passwords must be changed. JIS shall implement an appropriate change management process to ensure changes to systems are controlled by:

- Developing, documenting, and maintaining current baseline configurations.
- Network devices should be patched and updated for all security related updates/patches using automated tools when possible.

- Developing, documenting, and maintaining current inventories of the components of information systems and relevant ownership information.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and provide the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.
- Maintaining backup copies of hardened system configurations.

6.3 Service Interface Agreements

With the exception of 'NetworkMaryland' provided connections, external network connections shall be permitted only after all approvals are obtained consistent with this Policy and shall be managed as agreed to by the Judiciary and the untrusted entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system that includes:

- Purpose and duration of the connection as stated in the agreement, lease, or contract.
- Points-of-contact and cognizant officials for both the Judiciary and untrusted entities.
- Roles and responsibilities of points-of-contact and cognizant officials for both Judiciary and untrusted entities.
- Security measures to be implemented by the untrusted organization to protect the Judiciary's IT assets against unauthorized use or exploitation of the external network connection.
- Requirements for notifying the JIS Information Security Senior Manager within two business days of a security incident on the network.

6.4 Contingency Planning

JIS shall develop, implement, and test an IT Disaster Recovery plan for all systems determined to be essential for ongoing business operations. Creation, maintenance, and annual testing of a plan will minimize the impact of recovery and loss of information assets caused by events ranging from a single disruption of business to a disaster. Disaster Recovery plan maintenance should be incorporated into the JIS change management process to ensure plans are kept current.

Primary Components of an IT Disaster Recovery plan are:

- Identification of a disaster recovery team
- Definitions of recovery team member responsibilities
- Documentation of each critical system including:
    - Purpose
    - Hardware
    - Operating System
    - Application(s)
    - Data
    - Supporting network infrastructure and communications
- System restoration priority list
- Description of current system back-up procedures
- Description of back-up storage location

- Description of back-up testing procedures (including frequency)
- Identification of disaster recovery site including contact information
- System Recovery Time Objective RTO
- System Recovery Point Objective RPO (how current the data should be)
- Procedures for system restoration at backup and original JIS site

6.5 Incident Management

Incident Management refers to the processes and procedures JIS implements for identifying, responding to, documenting and managing information security incidents. A security incident within the JIS managed networks is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices.

6.6 Maintenance

JIS must identify, approve, control, and routinely monitor the use of information system maintenance tools and remotely executed maintenance and diagnostic activities. Only authorized personnel are to perform maintenance on information systems.

JIS must ensure that system maintenance is scheduled, performed, and documented in accordance with manufacturer or vendor specifications and this Policy.

6.7 Media Protection

The purpose of this section is to ensure proper precautions are in place to protect confidential information stored on media.

JIS shall restrict access to system media containing confidential information to authorized individuals. Media containing confidential information shall be physically controlled and securely stored. JIS must protect and control confidential system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Throughout the lifecycle of IT equipment, there are times when JIS will be required to relinquish custody of the asset. The transfer of custody may be temporary, such as when equipment is serviced or loaned, or the transfer may be permanent; examples being a donation, trade-in, lease termination or disposal.

To eliminate the possibility of inadvertently releasing residual Judiciary confidential information, the Judiciary will have a formal procedure for media sanitization.

6.8 Physical and Personnel Security

Physical access to information technology processing equipment, media storage areas, and mass media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized access to these areas.

The Judiciary must:

- Secure IT areas with controls commensurate to the risks
- Ensure secure storage of media
- Obtain personnel security clearances where appropriate

Physical access controls must be in place for the following:

- Data Centers
- Areas containing production servers
- Networking cabinets and wiring closets
- Power and emergency backup equipment

Access to data centers and secured areas should be limited to those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas.

Authorization should be:

- Based on frequency of need for access.
- Approved by the Administrative Official responsible for the secured area.

The Administrative Official or designee for each data center or secured area is responsible for:

- Ensuring that all removable media are physically secured.
- Ensuring proper employee/contractor identification processes to include periodic recertification are in place.
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems.
- Ensuring that any physical access controls are auditable.

6.9 System and Information Integrity

JIS shall implement system and information integrity security controls including vulnerability remediation, information system logging and monitoring, information input restrictions and information output handling and retention.

JIS must protect against malicious code, virus or malware by implementing procedures and solutions that, to the extent possible, includes a capability for automatic updates. Intrusion detection/prevention tools and techniques must be employed to log, monitor and review system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

JIS systems must restrict information input to authorized personnel (or processes acting on behalf of such personnel) responsible for receiving, processing, storing, or transmitting confidential information.

Information system security alerts/advisories for critical software must be regularly reviewed and applied as appropriate by the person(s) assigned responsibility for software administration.

Periodic external and internal vulnerability assessments must be performed to verify security controls are working properly and to identify risks.

6.10 System Development Life Cycle Methodology

All Judiciary systems must include IT security as part of the system development life cycle (SDLC) management process. This process must include:

- Implement requirements for ensuring authenticity and protecting message integrity in applications.
- Implement processes to control the installation of software on operating systems.
- Implement procedures to select, protect and control test data. Do not use test data in a production environment or use production data in a test environment without careful consideration.
- Limit access to program source code and place source code in a secure environment.
- Implement change/configuration control procedures to minimize the corruption of information.

SECTION 7: Technical Level Controls

7.1 Access Control Requirements

- The Judiciary must manage user accounts, including activation, deactivation, changes and audits.

- The Judiciary must ensure that only authorized users (employees or agency contractors) have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of “least possible privilege” and “need to know”.

- The Judiciary must ensure that systems or business processes, where feasible, enforce separation of duties through assigned access authorizations.

- Information systems must display the approved use agreement before granting system access.

- JIS must ensure that unauthorized users are denied access by ensuring that user sessions time out or initiate a re-authentication process after an approved period of inactivity.

- JIS must authorize, document, and monitor all remote access capabilities used on its systems. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption for transmission of data and authentication information.

- JIS must develop formal procedures for authorized individuals to access its information systems using a remote connection.

- JIS must authorize, document, and monitor all wireless access to its information systems. Wireless security guidelines are documented in Section 15.

7.2 Audit & Accountability Control Requirements

- The following minimum set of events/actions on systems that are categorized as critical or confidential, shall be logged and kept as required by all applicable State and Federal laws or regulations:
    - Additions, changes or deletions to data produced by the system
    - Authentication and Authorization processes
- A process must be established to detect and where feasible, alert the responsible parties in the event of an audit processing failure and appropriate remediation steps must be taken.
- Information systems must be configured to allocate sufficient audit record storage capacity to record all required auditable items.
- Procedures must be developed to routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to responsible parties for prompt resolution.
- To support the audit of activities, JIS must ensure that audit information is archived for the lesser of 3 years or unless otherwise requested by an Internal or External Audit Agency, legal requirement, or as directed by AOC Executive Management.
- JIS must protect audit information and audit tools under its control from unauthorized access, modification, and deletion.

7.3 Authentication & Authorization Control Requirements

- Users, devices, and processes must use standard authentication via the assignment of unique user accounts using standard authentication methods such as passwords, tokens, etc.
- Each user is responsible for all activities performed using his/her account credentials.
- Each user is responsible for their assigned account. Users are prohibited from sharing their account credentials with others, including other Judiciary personnel except as otherwise provided by policy (see Exhibit 1).
- Users must validate their identity when requesting a password reset or account unlock. The validation process must be at least as strong as when originally established.
- Shared functional accounts are prohibited unless formal approval is obtained from JIS Information Security.
- All requests for accounts must follow the formal documented procedures.
- The Judiciary must manage user accounts assigned within its information systems. Effective user account management practice includes:
    - Obtaining authorization from appropriate officials to request user account creation,

modification and deletion.

- Performing periodic recertification of application users and their associated privileges based on level of sensitivity.
- Timely disablement of user accounts when no longer required.

- Information Systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

7.4 User Authentication & Password Requirements

Passwords must meet the following construction, usage and change requirements:

- The password must not be the same as the user id
- Passwords must not be stored in clear text
- System design must prohibit or obfuscate password display during entry of clear text passwords
- Temporary passwords must be changed at the first logon
- Passwords must be complex to the extent possible supported by the system (e.g., contain a combination of at least three of the following four elements: upper case letter, lower case letter, number, or special character)
- User-level passwords must be changed at required intervals
- Password reuse must be prohibited by not allowing reuse of the last 'n' passwords, where 'n' is a number (e.g., 10) defined in the system password configuration
- User ids associated with a password must be locked after a specified number of failed login attempts
- User ids associated with a password must be automatically disabled or locked after a specified period of account inactivity
- User's identity must be validated when a user password reset is requested

System exceptions to user authentication and password requirements must be formally approved and documented.

Functional/System accounts may have unique authentication and password requirements that cannot comply with these requirements. Mitigating security controls must be in place that reduces risk to an acceptable level. These controls must be formally approved and documented.

7.5 System & Communication Control

- Information systems shall separate front end interfaces from back end processing and data storage, where feasible.

- Information systems shall prevent unauthorized and unintended information transfer via shared system resources by adhering to the concept of least privilege and ensuring functional accounts are not shared across applications.

- Information systems shall be configured to monitor and control communications at the external boundaries of the information systems and at key internal boundaries within the systems.

- Information systems must protect confidential information during electronic transmission. The Judiciary must secure all confidential information during transmission.

- When Public Key Infrastructure (PKI) is used, JIS shall establish and manage cryptographic keys using secure mechanisms with supporting procedures.

- Whenever there is a network connection external to the system, the information system shall terminate the network connection at the end of a session or after an approved period of inactivity.

SECTION 8: Virtualization Technologies

JIS must install, configure and deploy virtualization solutions to ensure that the virtual environment is as secure as a non-virtualized environment and in compliance with all relevant JIS Policy and Procedures.

SECTION 9: Cloud Technologies

Judiciary implementation of a cloud-based solution must be implemented to ensure the solution is as secure as on premise and is in compliance with relevant JIS Security Policy and Procedures.

SECTION 10: Information Systems Contracts

Contracts shall be written to ensure vendor agrees to adhere to JIS Security Policy and Procedures and all applicable Rules, State and Federal laws or regulations.

SECTION 11: Mobile Devices

Any user receiving Judiciary data or connecting a mobile device to the Judiciary network must comply with the JIS Security Policy and Procedures and all applicable Rules, State and Federal laws or Regulations.

SECTION 12: General Computer and Network Use Policy

All users of Judiciary information systems must acknowledge and comply with the General Computer and Network Use Policy and are bound to modifications as posted to this document.

SECTION 13: Data Loss Prevention Guidance

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use, data in motion and data at rest. DLP controls are based on policy and include classifying sensitive data, discovering that data across an enterprise, enforcing controls and reporting and auditing to ensure policy compliance. A comprehensive DLP solution should include the following controls:

- Use network monitoring tools to analyze outbound traffic looking for anomalies which may include; large file transfers, long-time persistent connections, connections at regular repeated intervals, unusual protocols and ports in use, and possibly the presence of

certain keywords in the data traversing the network perimeter.

- Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting appropriate personnel.

- Use outbound proxies to monitor and control all information leaving the Judiciary.

- Use secure, authenticated, or encrypted mechanisms to move confidential data between untrusted networks.

- Confidential data stored on removable and easily transported storage media such as USB media and CDs/DVDs must be secured.

SECTION 14: Software Licenses and Use

Unless specifically approved by the Assistant Administrator of JIS, a user's personal or a contractor's business IT equipment shall not have Judiciary proprietary or licensed software installed and shall not be used to process or transmit proprietary or confidential information. Only Judiciary owned and authorized computer software is to be used on Judiciary owned machines. Users are not authorized to install their own software.

All users of Judiciary information systems must comply with copyright laws.

SECTION 15: Wireless Security

Policies and Procedures supporting the use of wireless technology used in the JIS managed network shall:

- Establish a process for documenting all wireless access points.

- Ensure proper security mechanisms are in place to prevent the theft, alteration or misuse of access points, introduction of rogue devices or access to the Judiciary network.

- Restrict hardware to Wi-Fi certified devices that are configured to use the latest security features available.

- Change default administrator credentials.

- Change default SNMP strings if used, otherwise disable SNMP.

- Change default SSID.

- Deploy secure access point management protocols and disable telnet.

- Strategically place and configure access points to minimize SSID broadcast exposure beyond the physical perimeter of the building.

- Require wireless users to provide unique authentication over encrypted channels if

accessing internal LAN services.

- Require wireless users to utilize encrypted data transmission if accessing internal LAN services.