FLORIDA DEPARTMENT OF LAW ENFORCEMENT
Contract FDLE-005-19

This Contract, by and between CutCom Software Inc. d/b/a AppArmor, a company duly authorized to conduct business with the State of Florida, whose business address is 545 King Street West, Toronto, Ontario, Canada M5W 1A2 (hereinafter referred to as Contractor), and the State of Florida's Department of Law Enforcement, (hereinafter referred to as FDLE).

WITNESSETH THAT:

WHEREAS, FDLE issued Solicitation Number FDLE 1833 and the Contractor submitted a reply to Invitation to Negotiate, FortifyFL Reporting System and;

WHEREAS, Contractor desires to enter into a Contract with FDLE to provide certain products and services; and

WHEREAS, FDLE desires to enter into a Contract with Contractor in order to acquire certain Contractor supplied products and services;

NOW THEREFORE, Contractor and FDLE for and in recognition of considerations hereinafter set forth, do hereby agree as follows:

This Contract shall be comprised of the following documents, attachments, addenda and any subsequent amendments to this Contract. These documents, attachments, addenda and amendments shall govern the services provided by the Contractor and are hereby incorporated in, and are made a part of, this Contract. The order of precedence is as indicated below. Subsequent amendments take first precedence, with the most current documents or updates of the documents controlling in the event of a conflict between differing versions of a document which form part of or are incorporated in this Contract.

The documents specified below are hereby incorporated in, and are a part of this Contract, including this document, captioned “Contract FDLE-005-19” which shall be first in order of precedence:

- Contract FDLE-005-19;
- Attachment A – FDLE Scope of Work (Revised);
- CONTRACTOR Best and Final Offer and CONTRACTOR’s Original Technical Response (Attachment B);
- FDLE ITN 1833 final document, terms and conditions (incorporated herein by reference); and
- Contractor’s Software Configuration and Support Agreement (Attachment C);

1. Contract Term

The term of this Contract shall begin from the last date signed by the parties below and continue for a period of three (3) years. At the option of the Department, the term may be renewed for three (3) additional years, by exercising up to three (3) one (1) year renewal options.

2. Deliverables

CONTRACTOR shall provide all services, products and capabilities identified in the Attachment A Statement of Work, Attachment B CONTRACTOR Best and Final Offer / Original Technical Response, and the FDLE ITN 1833 final documents to configure, implement and support the FortifyFL Reporting System.

Major Deliverable	**Performance Metric**
<u>Implementation</u>: 1) Requirements Validation Document (RVD) and Project Plan. 2) Pilot Group Testing and Development Deployment 3) Administrator Training 4) Product Deployment 5) System Acceptance	Implementation deliverables are fixed rate as described in the Statement of Work (SOW). Upon successful completion of activities described in each deliverable, payment(s) will be processed and approved upon written acceptance of work product(s) by the FDLE ITS Project Manager.
<u>Annual Subscription / License Fee</u>	Premium Software support for the FortifyFL mobile safety and reporting application for smartphones, and State of Florida webpage crime reporting tool.

The submission of a completed **Deliverable Acceptance Form** (**Appendix A**) to the Contractor will initiate invoice for payment of that deliverable to the Department, in accordance with the Deliverable Acceptance Process in Attachment A, Section I (C).

3. Contract Price

System implementation and three (3) year annual subscription / license fees to include all proposed features are firm fixed pricing in accordance with the AppArmor Best and Final Offer (Attachment A):

Implementation of the FortifyFL System	**Price**
1) RVD and Project Plan	$20,700
2) Pilot Group Testing and Development Deployment	
3) Administrator Training	$20,700
4) Production Deployment	
5) System Acceptance	$41,400
Implementation Sub-Total	**$82,800**
Year One (1) Annual Subscription / License Fee	$ 57,200
Year Two (2) Annual Subscription / License Fee	$ 57,200
Year Three (3) Annual Subscription / License Fee	$ 57,200
Total Contract Value	**$254,400**

Additional features not included in the firm fixed pricing but offered in accordance with the AppArmor Best and Final Offer may be included at any time during the initial implementation phase, or at any time during the base contract term or renewal year options, with final pricing subject to negotiation prior to implementation.

FLORIDA DEPARTMENT OF LAW ENFORCEMENT STANDARD TERMS AND CONDITIONS

1. PUR 1000 – General Contract Conditions

https://www.dms.myflorida.com/content/download/2933/11777/PUR_1000_General_Contract_Conditions.pdf
The State of Florida General Terms and Conditions (PUR 1000) are hereby referenced and incorporated in their entirety into this ITN. This is a downloadable document. Potential Respondents to the solicitation are encouraged to carefully review all materials contained herein and prepare Replies accordingly. The Florida Department of Law Enforcement Standard Terms and Conditions supersedes any contract condition otherwise duplicated herein.

2. American with Disabilities Act (ADA) Civil Rights Compliance

CONTRACTOR represents and warrants that it will comply with all Equal Accessibility laws, regulations and standards under Sections 251 & 255 of the Telecommunications Act of 1996, Titles I, II, III & IV of the Americans with Disabilities Act (ADA) [42 USC 12101 et seq.], and Sections 504 and 508 of the Federal Rehabilitation Act amendments [29 USC 794 et seq.], and the Assistive Technology Act of 1998. These standards establish a minimum level of accessibility.

Contractor will indemnify the customer against any litigation stemming from a lack of compliance with the above laws, regulations and standards.

3. Change Management

The Department will coordinate and lead project change control activities. This will include documentation of change requests that will describe the nature and scope of changes, justification for changes, and the expected impacts of the request on the project schedule and budget. Change requests will be associated with a previously raised Issue or Risk that is documented. All change requests will be tracked by the FDLE Program Manager and FDLE Project Manager throughout the life of the project, regardless of status.

By way of example, and without limitation, changes may include the following:

- Any activities not specifically set forth in this SOW
- Providing or developing any deliverables not specifically set forth in this SOW
- Change in requirements as stated or referenced by this SOW
- Any change in the respective responsibilities of Contractor and Department set forth in this SOW, including any reallocation or any changes in engagement or project staffing
- Any rework of accepted/approved deliverables

A scope change is defined as a change to the original boundaries of the project, as defined by the contract and this SOW, which changes the budget, schedule and/or contract requirements. Scope changes will be identified at the start of the change management process.

Change Request Initiation: Project change requests to this SOW may be initiated by the Department or the Contractor. Project change requests will be documented in writing and must identify cost and schedule, and contain a justification or statement of need for the requested changes. The FDLE Project Manager will assign a change request number.

Change Impact Estimation: Each project change request must be reviewed by the Contractor, FDLE Program Manager, and FDLE Project Manager to decide whether to proceed with the requested changes. The Contractor will evaluate the impact of project change requests to determine impact on scope, schedule, and cost and provide any other necessary details. For change requests impacting scope, schedule, or cost, the Contractor will submit to the FDLE Program Manager and FDLE Project Manager a written estimate based on this evaluation.

Approvals and Acceptance: The Department may, at its sole discretion, approve or decline a change request. Only those project change requests that have been approved in writing by both the Contractor and Department will be considered authorized changes. No request for alteration, modification or additional work affecting the scope, schedule, or cost will be valid unless the resulting change has been approved by the Department in the form of a contract amendment.

Change Management Review Process: The Contractor will submit a formal change request to the FDLE Project Manager using the **Change Request Form** (**Appendix B**). Any additional materials the Contractor submits with the change request will be noted as attachments.

The change request will be reviewed by the FDLE Program Manager, FDLE Project Manager, and FDLE Executive Management, if applicable. The FDLE Program Manager and FDLE Project Manager will determine how much time is required to analyze the change request. The timeframe for the Department's review and analysis of change requests will be dependent on the extent of the modification requested and due date(s) of impacted deliverable(s).

The analysis associated with the Project Change Request will include the business benefit, implications if the change is not made, impacts to the project (including budget, schedule, and/or contract requirements), as well as alternatives. The Department will communicate anticipated review schedules with the Contractor based on the requirements of each change request.

All project change requests impacting cost, schedule or scope must be referred to FDLE Executive Management for approval. Once analysis has been completed, the FDLE Program Manager and FDLE Project Manager will present the results and recommendation for the request to FDLE Executive Management for written approval.

The Contractor will be notified in writing of the decision of all change requests. Based on the resolution or recommended course of action, the FDLE Project Manager or Contract Manager will make any required modifications to the agreement and/or Appendices.

If FDLE Executive Management decides not to proceed with the change or an alternative, then the FDLE Project Manager will inform Contractor in writing. FDLE Executive Management can close a change request, but suggest that it be reviewed later. The FDLE Project Manager will include a review of the open change requests at Project Status Review.

4. Compliance with Laws

The Contracting Party shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of Federal, State, and local agencies having jurisdiction and authority. Violation of such laws may be grounds for contract termination.

5. Confidential Information

Confidential Information" means information or materials provided by one party to the other which are: i) in tangible form and labeled "confidential" or the like; ii) if disclosed orally, are identified as being confidential at the time of disclosure; or iii) such that a reasonable person would consider it confidential from the nature of the information and circumstances of disclosure. The receiving party will hold the Confidential Information in strict confidence, will use it only for purposes of this Contract, and disclose it only to employees and agents who have a need to know such Confidential Information and who have agreed to abide by the terms of this Section prior to disclosure. The receiving party will exercise the same care in preventing the unauthorized disclosure or use of the Confidential Information that it takes to protect its own information of a similar nature, which in no event will be less than reasonable care. The restrictions on the use and disclosure of Confidential Information specified hereunder will not apply to information: (i) which is independently developed by the receiving party or lawfully received from another source without breach of this Contract; (ii) which is or becomes generally available to the public without breach of this Contract by the receiving party; (iii) which at the time of disclosure was known to the receiving party; (iv) which is disclosed to unaffiliated third Parties without restriction by the disclosing party; or (v) which is disclosed pursuant to law, judicial order, or government regulations so long as the receiving party promptly notifies the disclosing party prior to disclosure and cooperates with the disclosing party in the event that the disclosing party elects to contest or avoid such judicial or governmental disclosure, whether by seeking a protective order or otherwise. FDLE information which is made confidential or exempt from disclosure by law will retain that status notwithstanding the occurrence of the specified exceptions to restrictions on use and disclosure, to the extent permitted by law. FDLE agrees to maintain the confidentiality of Confidential Information, as that term is used in this Contract, received from CONTRACTOR, to the extent this can be accomplished without violating Florida Law regarding public records, as set forth in Chapter 119, Florida Statutes. In particular, FDLE agrees to maintain the confidentiality of Confidential Information to the extent such information constitutes Trade Secret Information, as that term is used in Section 815.045, Florida Statutes, and as defined at Section 812.081(1)(c), Florida Statutes.

All data, including statistical information and reports, provided to the Contractor, or generated as a result of this Contract will remain the exclusive property of FDLE and may not be copied, published or removed by Contractor agents and subcontractors, without the express written permission of FDLE.

CONTRACTOR is responsible for the actions of its agents and subcontractors with respect to protection of confidential law enforcement and other types of confidential data.

6. Contracting Party Employees, Subcontractors, and Other Agents

Contracting Party will be an independent contractor, and not the agent or servant of the Department and will not be entitled to any benefits granted employees of the State of Florida. The Department and the State shall take all actions necessary to ensure that Contracting Party's employees, subcontractors and other agents are not employees of the State of Florida. Such actions include, but are not limited to, ensuring that Contracting Party's employees, subcontractors, and other agents receive benefits and necessary insurance from an employer other than the State of Florida. Each party agrees to assume complete responsibility for its own employees with regard to federal or state employers' liability and withholding tax, worker's compensation, social security, unemployment insurance, and Occupational Safety and Health Administration requirements and other federal, state and local laws.

The Contracting Party will have complete supervision and control over its own agents, servants and employees. The Contracting Party will ensure that personnel of any agent or subcontractor are trained, qualified, and available to perform the services for which they are contracted to perform.

The Contracting Party is responsible for managing the relationship with all subcontractor organizations, for directing and managing the work efforts of subcontractor personnel, and for the quality of the work of subcontractor personnel. Upon request, Contracting Party shall furnish a copy of technical certification or other proof of qualification. All employees, subcontractors, or agents performing work under the contract must comply with all security and administrative requirements of the Department and shall comply with all controlling laws and regulations relevant to the services they are providing under the contract.

7. Controlling Law

All matters, whether sounding in tort or contract, relating to the validity, construction, interpretation, performance and enforcement of this contract shall be determined by the laws of the State of Florida. The exclusive venue of any legal or equitable action that arises out of or relates to the contract shall be the appropriate state court in Leon County, Florida; in any such action, Florida law shall apply and the parties waive any right to jury trial.

8. Contractor’s Responsibilities under Termination

After receipt of notice of termination, and except as otherwise specified by the Department, the Contractor shall (i) stop work under this Contract on the date, and to the extent specified, in the notice; (ii) place no further order(s) or subcontract(s) for materials, services, or facilities except as may be necessary for completion of such portion of the work under this Contract that is not terminated; (iii) complete performance of such part of the work as shall not have been terminated by the Department; and (iv) take such action as may be necessary, or as the Department may specify, to protect and preserve any property or data related to this contract which is in the possession of the contractor(s) and in which the Department has or may acquire an interest.

Upon the effective date of termination of the Contract, the Contractor shall transfer, assign, and make available to FDLE all property, materials, and data belonging to the Department, all rights and claims to any and all reservations, contracts and arrangements with subcontractors, or others, and shall make available to the Department all written information regarding the performance of the Contract . Any data transferred shall be in a format specified by the Department. No extra compensation will be paid to the Contractor for its services in connection with such transfer or assignment. The Department concurrently with such transfer or assignment reserves the option to assume the obligations of the Contractor if any, on all non- cancelable contracts with third parties.

9. Discrimination

In the performance of such services, the Contracting Party agrees not to discriminate against any employee or applicant for employment on grounds of race, creed, color, sex, age, national origin, or disability.

10. Dispute Resolution

Any dispute concerning performance of the Contract which cannot be resolved by informal discussion between the FDLE and the Contractor will be referred to negotiation to be conducted by the FDLE General Counsel. If FDLE and Contractor's representatives are unable to resolve the dispute within five (5) business days after commencing negotiations, or fifteen (15) calendar days have passed since the initial request for negotiations at this level, then the Parties will be entitled to discontinue negotiations, to seek to resolve the dispute through mediation as hereinafter provided or, if the Parties do not agree to submit the dispute to non- binding mediation, to seek any and all rights and remedies that may be available under this Contract, at law or in equity.

Mediation must occur within twenty (20) business days after the Parties agree to submit the dispute to mediation. The Parties mutually will select an independent mediator experienced in IT systems and services Contracts, and each will designate a representative(s) to meet with the mediator in good faith in an effort to resolve the dispute. The specific format for the mediation will be left to the discretion of the mediator and the designated Party representatives and may include the preparation of agreed-upon statements of fact or written statements of position furnished to the other Party. If the Parties are unable to resolve a dispute through the dispute resolution processes described in this Section, then either party may seek any and all rights and remedies that may be available under this Contract, at law or in equity.

All Contractor obligations related to project activities and support services under this Contract will continue without interruption during disputes unless suspended by FDLE or unless the dispute relates to non-payment by FDLE. FDLE reserves the right to withhold payments during disputes relating to breach by Contractor. The failure of FDLE to release payment during disputes relating to breach by Contractor will not constitute a breach or default by FDLE.

11. Documentation in Escrow

The Contractor agrees to keep and maintain current one copy of the Licensed Program source code with an escrow agent approved by the Department. The source code shall be maintained in a secure location.

The Contractor represents and warrants that the source code is and shall be understandable and useable by a trained computer-programming \ contractor who is generally familiar with the programming language(s) used to produce the Licensed Program. Contractor further represents and warrants that the licensed software programs do not involve any proprietary languages or programming components that such a contractor could not reasonably be expected to understand, except to the extent the source code contains sufficient commentary to enable such contractor to understand and use such languages or components. Contractor further represents and warrants that the Source Code includes all of the devices, programming, and documentation necessary for the maintenance of the Licensed Program by the Department upon release of the source code pursuant to this Contract, except for devices, programming, and documentation commercially available to the licensee on reasonable terms through readily known sources other than the Contractor.
The Contractor agrees that the Department may access and the escrow agent may release the source

code and Supporting Documentation, which has been brought up to date continuously, upon the occurrence of any of the following events (nonexclusive list):

- Inability of the Contractor to provide maintenance under this Contract.
- The Contractor declares bankruptcy or ceases to do business.

The Contractor will maintain current one copy of Supporting Documentation which is required for the proper maintenance of the licensed software with the escrow agent. Such documentation will consist of Coding Instructions, Installation Instructions, and Maintenance and Technical Support manuals, and will be the same as that which the Contractor supplies to its technical personnel to maintain the licensed software.

Upon taking possession thereof, the Department agrees that all information disclosed to the Department by the Contractor will be held in confidence and will be used only in performance or maintenance of the Licensed Programs. The Department shall exercise the same standard of care to protect such information as is used to protect its own proprietary data.

12. Effective Date

This Contract shall be effective when signed by the Contracting Party and the Department.

13. Execution in Counterparts

The Contract may be executed in counterparts, each of which shall be an original and all of which shall constitute but one and the same instrument.

14. E-Verify

The Department shall consider the employment by any Contractor of unauthorized aliens a violation of section 274(e) of the Immigration and Nationalization Act. Such violation shall be cause for unilateral cancellation of this Contract. The Contracting Party certifies that it participates in the U.S. Department of Homeland Security's E-Verify Employment Eligibility Verification Program, and that it will assure that any sub-contractor with which it contracts for the performance of this contract participates in the E-Verify Employment Eligibility Verification Program.

15. Financial Consequences

If the Contracting Party fails to meet the minimum level of service or performance identified in this Contract, or is customary for the industry, then the Department will apply financial consequences. Financial consequences may include but are not limited to withholding payments until the deficiency is cured, withholding one and one-half percent (1.5%) of the Deliverable fee specified in the Contract for each day that the deliverable is late, imposition of other financial consequences and termination of contract and requisition of goods or services from an alternate source. Any payment made in reliance on Contracting Party’s evidence of performance, which evidence is subsequently determined to be erroneous, will be immediately due to the Department as an overpayment.

16. Force Majeure, Notice of Delay, and No Damages for delay

Contractor will not be responsible for delay resulting from its failure to perform if neither the fault nor the negligence of Contractor or its employees or agents contributed to the delay and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, severe disruption of the FDLE CJNet or other network, or other similar cause wholly beyond Contractor's control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to Contractor. In case of any delay Contractor believes is excusable, Contractor will notify FDLE in writing of the delay or potential delay and describe the cause of the delay either (1) within ten (10) days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result, or (2) if delay is not reasonably foreseeable, within five (5) business days after the date Contractor first had reason to believe that a delay could result. THE FOREGOING WILL CONSTITUTE CONTRACTOR'S SOLE REMEDY OR EXCUSE WITH RESPECT TO DELAY FOR A FORCE MAJEURE EVENT. Providing notice in strict accordance with this paragraph is a condition precedent to such remedy. No claim for damages, other than for an extension of time, will be asserted against the FDLE as a result of a force majeure event. Contractor will not be entitled to an increase in the Contract price or payment of any kind from FDLE for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of delay, disruption, interference, or hindrance from a force majeure event. If the delay, disruption, interference, or hindrance is caused by FDLE, the Change Management process provided will be invoked, with necessary adjustments to the scope, schedule or cost of the project as agreed to by the parties. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist, Contractor will continue to perform under this Contract, unless the Contract is renegotiated or terminated by agreement of the Parties, or terminated by FDLE

Contractor shall not be subject to a claim of default or termination, to the extent such failure is due to:

i) force majeure events as defined in this Section; ii) failures by FDLE or its agents to make necessary decisions or to perform any responsibilities under this Contract that were required for Contractor meet its performance obligations under this Contract (for example, failure by FDLE to comply with the review times prescribed in the Statement of Work, Submission, Review, and Acceptance Process, failure to timely install essential hardware or equipment through no fault of Contractor); iii) acts or omissions of a party other than Contractor or its subcontractors; or iv) errors or defects in FDLE's equipment, facilities, software and retained functions.

17. Insurance Requirements

During the Contract term, the Contracting Party at its sole expense shall provide commercial insurance of such a type and with such terms and limits as may be reasonably associated with the contract. Providing and maintaining adequate insurance coverage is a material obligation of the Contracting Party. Upon request, the Contracting Party shall provide certificate of insurance. The limits of coverage under each policy maintained by the Contracting Party shall not be interpreted as limiting the Contracting Party's liability and obligations under the contract. All insurance policies shall be through insurers authorized or eligible to write policies in Florida.

18. Intellectual Property

The parties do not anticipate that any intellectual property will be developed as a result of this contract. However, any intellectual property developed as a result of this contract will belong to and be the sole property of the state. The rights conveyed to the state pursuant to this Agreement do not include rights to any preexisting Intellectual Property used, developed and refined by the Contracting Party and its subcontractors during their provision of Services under this Agreement. This provision will survive the termination or expiration of any contract.

19. Invoicing

All invoices or bills for fees or other compensation for services, or expenses shall be submitted with reasonable detail for a proper pre-audit and post-audit thereof, to comply with Section 287.058(1) (a), Florida Statues. This information will include Contractor Name and remit to address; Contractor billing contact phone number and/or email address; Contractor FEID number; Contract number; Month/Year Billing term; detailed deliverable number with description; and payment amount due.

Invoices must be submitted to:

Florida Department of Law Enforcement
Attn: Accounts Payable
P.O. Box 1489
Tallahassee, FL 32308
Phone: 850-410-7155
Email: fdleaccountspayable@fdle.state.fl.us

Whenever this Contract is terminated with or without cause, all amounts due shall be pro-rated.

20. The Department is Self-Insured

The Department is self-insured for its torts to the extent provided in Section 768.28, Florida Statutes, to cover bodily injury, death and property damage arising as a consequence of the acts and omissions to act of its officers, employees, and agents. The Department is without authority to insure the contracting party in any way. The Department shall not be deemed to assume any liability for the acts, omissions to act and negligence of the Contracting Party, its agents, servants and employees; nor shall the Contracting Party exclude liability for its own negligence to the Department or any third party, except as allowed by law and agreed to by the Department. The Department is without authority to indemnify or hold harmless the Contracting Party.

Unless authorized by law and agreed to in writing, the Department shall not be liable to pay attorney fees, interest, late charges and service fees and/or costs of collection.

21. Modification of Terms

The Contract contains all the terms and conditions agreed upon by the parties, which terms and conditions shall govern all transactions between the Department and the Contracting Party and any communications, promises, representations or agreements, not included in writing in this contract, shall not be binding upon any party. The Contract may only be modified or amended upon mutual written agreement of the Department and the Contracting Party. No oral agreements or representations shall be valid or binding upon the Department or the Contracting Party. No alteration or modification of the Contract terms, including substitution of product, shall be valid or binding against the Department. The Contracting Party may not unilaterally modify the terms of the Contract by affixing additional terms to product upon delivery (e.g., attachment or inclusion of standard preprinted forms, product literature, “shrink wrap” terms accompanying or affixed to a product, whether written or electronic) or by incorporating such terms onto the Contracting Party’s order or fiscal forms or other documents forwarded by the Contracting Party for payment. The Department's acceptance of product or processing of documentation on forms furnished by the Contracting Party for approval or payment shall not constitute acceptance of the proposed modification to terms and conditions.

22. Non-Material Errors

CONTRACTOR and FDLE agree that non-material errors in contract language, terms and conditions (e.g., typos and other obvious errors) will be correctable without amending the Contract provided that the nature of the Contract is not altered by such correction.

23. Limited Offshoring Affidavit

The Contractor is hereby authorized to perform services under the Contract from its headquarters in Ontario, Canada. The Contractor is further hereby authorized to send, transmit or access State of Florida Data from its headquarters in Ontario, Canada in performance of this Contract. Access to the State of Florida Data will be restricted to Contractor staff who are assigned to State of Florida, FortifyFL account. Outside of the aforementioned exceptions, Contractor will not otherwise allow any State of Florida Data to be sent by any medium, transmitted or accessed outside of the United States.

The Contractor agrees that a violation of items listed above will result in immediate and irreparable harm to the Department and will entitle the Department to a credit of $50,000 per violation, with a total cap of $500,000 per event. This credit is intended only to cover the Department’s internal staffing and administrative costs as well as the diminished value of Services provided under the Contract and will not preclude the Department from recovering other damages it may suffer as a result of such violation. For purposes of determining the damages due hereunder, a group of violations relating to a common set of operative facts (e.g., same location, same time period, same off-shore entity) will be treated as a single event. A violation of this provision will also entitle the Department to recover damages, if any, arising from a breach of this section and constitutes an event of default.

Notwithstanding any provision of this Contract to the contrary, the Contractor shall notify the Department as soon as possible and in all events within one (1) business day in the event it discovers any Data is breached, any unauthorized access of State of Florida Data occurs (even by persons or companies with authorized access for other purposes), any unauthorized transmission of Data or any credible allegation or suspicion of a material violation of the above. This notification is required whether the event affects one employee/retiree or the entire population. The notification shall be clear and conspicuous and include a description of the following:
(a) the incident in general terms, (b) the type of personal information that was subject to the unauthorized access and acquisition, (c) the number of individuals who were, or potentially have been affected by the breach, and (d) the actions taken by the Contractor to protect the Data information from further unauthorized Access. However, the description of those actions in the written notice may be general so as not to further increase the risk or severity of the breach.

Upon becoming aware of an alleged security breach or security incident, the Contractor Security Officer shall set up a conference call with the Department’s Contract Manager. The conference call invitation shall contain a brief description of the nature of the event. When possible, a thirty (30) minute notice shall be given to allow Department personnel to be available for the call. If the designated time is not practical for the Department, an alternate time for the call shall be scheduled. All available information shall be shared on the call. The Contractor shall answer all questions based on the information known at that time and shall answer additional questions as additional information becomes known. The Contractor shall provide the Department with final documentation of the incident including all actions that took place. If the Contractor becomes aware of a security breach or security incident outside of normal business hours, the Contractor shall notify the Department's Contract Manager and in all events, within one (1) business day.

Upon execution of this Contract, the Contractor shall execute an Affidavit of Limited Offshoring. The **Affidavit of Limited Offshoring** (Appendix C) must be maintained throughout the Contract term and any renewals or extensions.

24. Non-Solicitation

Unless otherwise agreed to by the Parties in writing, during the term of the Contract and for a period of one (1) year after termination of the Contract, neither party, as between Contractor and, collectively, FDLE will directly or indirectly solicit, hire or otherwise retain as an employee or independent contractor a staff member of the other party or a former staff member that is or was involved with the Contract.

25. Notices

Whenever notice is required to be given by Certified Mail, Return Receipt Requested or private carrier express mail service, it shall be deemed to have been given on the date shown on the return receipt, or date of actual delivery, whichever is earlier.

Change of address, as well as, any other notice(s) required by this contract shall be delivered to the **Department of Law Enforcement** for the attention of:

The Office of General Services
2331 Phillips Road
Tallahassee, Florida 32308

And to the Contracting Party for the attention of:

Name:	David Sinkinson
Title:	Co-Founder of AppArmor
Street:	PO Box 12 Station A
Address:	Toronto, Ontario, Canada, M5W 1A2
Phone:	866-630-2251 x 179
Email:	dsinkinson@apparmor.com

26. Payment

The State of Florida cannot make deposits or pay for goods and/or services in advance unless approved under rules issued by the Florida Department of Financial Services. The Department is not authorized to pay to Contracting Party any deposit for services to be rendered or equipment to be purchased in the future.

Payment shall be made in accordance with Section 215.422, Florida Statutes, which states the Contracting Party's rights and the Department's responsibilities concerning interest penalties and time limits for payment of invoices. A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this individual include acting as an advocate for vendors who may be experiencing problems in obtaining timely payment(s) from a state agency. The Vendor Ombudsman may be contacted at 850-413-5516.

27. Public Records

This contract shall be unilaterally cancelled by the Department for refusal to allow public access to all documents, papers, letters or other material subject to the provisions of Chapter 119, Florida Statutes, and made or received in conjunction with the contract.

Pursuant to Section 119.0701, Florida Statutes, Contractor agrees to keep and maintain public records required by the FDLE to perform the service. Upon request from FDLE's custodian of public records, Contractor agrees to provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time, at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes.

The Contractor shall ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following the completion of the contract if the Contractor does not transfer the records to FDLE.

Upon completion of the contract, Contractor shall transfer, at no cost, to FDLE all public records in possession of Contractor or keep and maintain public records required by FDLE to perform the service. If Contractor transfers all public records to the public agency upon completion of the contract, the contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the contract, the Contractor shall meet all applicable requirements for retaining public records, in a format that is compatible with the information technology systems of FDLE.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT 850-410-7676, PUBLICRECORDS@FDLE.STATE.FL.US, OR VIA MAIL AT P.O. BOX 1489, ATTN: PUBLIC RECORDS DIVISION, TALLAHASSEE, FL 32302.

The Contractor agrees to the provisions of Section 287.057(16), Florida Statutes, and shall maintain throughout the term of the contract and at least four (4) years thereafter, detailed current records, including documentation of all expenses, disbursements, charges, credits, underlying receipts and invoices. All such records shall be made available for inspection and copying upon request in accordance with Chapter 119, Florida Statutes.

In accordance with Section 215.985(16), Florida Statutes, this contract is subject to inclusion in the Florida Public Accountability Tracking System (FACTS) database and subject to posting, in whole or in part, on the Internet.

28. Right to Audit

Upon execution of the Contract, the Department reserves the right to conduct an audit of the Contractor's records pertaining to this project. The Department, the State, or their authorized representatives shall have access to such records for audit purposes during the term of this Contract and for five years following Contract completion.

29. Renewal

There shall be no automatic renewal of this contract. This Contract may be renewed for a period no longer than the original term of the contract. Renewal contracts may not include any compensation for costs associated with the renewal. Renewals shall be contingent upon satisfactory performance evaluations by the Department and subject to the availability of funds. FDLE reserves the option to not renew, upon the discovery of new technology.

30. Security Requirements and Confidentiality

The Contractor agrees to adhere to FDLE policies and procedures, State of Florida information security laws and rules, and FBI CJIS Security Policy. FDLE's Information Systems Security Addendum (Appendix D) provides more specific information security requirements for Contractor staff.

All agents and subcontractors with access to FDLE computer networks and systems to be engaged by the Contracting Party in the performance of this contract must be approved by FDLE and must abide by all applicable terms and conditions of the contract as well as FDLE security of information resources policies and procedures, State of Florida information security laws and rules.

Whenever necessitated by legitimate concern for reasonable security precautions as determined by the Department and without regard to the identity of any individual, the Department will require the Contracting Party(s) and/or employees of the Contracting Party(s) to submit to, and successfully pass, an appropriate security background investigation prior to being allowed access to any of the Department's facilities to perform those services as set forth in this contract. FDLE reserves the right to have Contracting Party's staff removed from the account when it is determined to be in the best interest of the State.

31. Severability

Any provision of this contract in violation of the laws of the State of Florida shall be ineffective to the extent of such violation, without invalidating the remaining provisions of this contract.

32. Survival

The provisions of all confidentiality obligations, indemnification, limitation of liability and any other sections, schedules or attachments to this Contract that by their nature may reasonably be presumed to survive any termination or expiration of this Contract, will so survive.

33. Suspension of Work

The Department may in its sole discretion suspend any or all activities under the contract or purchase order, at any time, when in the best interests of the State to do so. The Department shall provide the Contracting Party written notice outlining the particulars of suspension. Examples of the reason for suspension include, but are not limited to, budgetary constraints, declaration of emergency, or other such circumstances. After receiving a suspension notice, the Contracting Party shall comply with the notice for a period up to thirty (30) days after the notice is delivered to the Contracting Party, and for any further period to which the Parties may agree. Within thirty (30) days, or any longer period agreed to by the Contracting Party, the Department shall either (1) issue a notice authorizing resumption of work, at which time activity shall resume, or (2) terminate the contract or purchase order. Suspension of work shall not entitle the Contracting Party to any additional compensation.

34. Termination for Cause

The Department may terminate the contract if the Contracting Party fails to (1) deliver the product within the time specified in the contract or any extension, (2) maintain adequate progress, thus endangering performance of the contract, (3) honor any term of the contract, or (4) abide by any statutory, regulatory, or licensing requirement. Rule 60A-1.006(3), F.A.C., governs the procedure and consequences of default. The Contracting Party shall continue work on any work not terminated. Except for defaults of subcontractors at any tier, the Contracting party shall not be liable for any excess costs if the failure to perform the contract arises from events completely beyond the control, and without the fault or negligence, of the Contracting Party. If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is completely beyond the control of both the Contracting Party and the subcontractor, and without the fault or negligence of either, the Contracting Party shall not be liable for any excess costs for failure to perform, unless the subcontracted products were obtainable from other sources in sufficient time for the Contracting Party to meet the required delivery schedule. If, after termination, it is determined that the Contracting Party was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Department. The rights and remedies of the Department in this clause are in addition to any other rights and remedies provided by law or under the contract.

35. Termination for Convenience

This contract may be canceled in whole or in part by the Department when the Department determines in its sole discretion that it is in the Department's interest to do so upon giving 30 days written notice by Certified Mail, Return Receipt Requested or by private carrier express mail service. The Contracting Party shall not furnish any product after it receives the notice of termination, except as necessary to complete the continued portion of the Contract, if any. The Contracting Party shall not be entitled to recover any cancellation charges or lost profits.

36. Travel

It is not anticipated that the scope of this Contract will include travel compensation. Any travel related expense request must be submitted and obtain prior approval by the FDLE. All bills for any travel expenses that are authorized by Section 112.061, Florida Statues, shall be submitted and paid in accordance with the rates specified in Section 112.061, Florida Statutes, governing payments by the State for travel expenses.

37. Waiver

No delay or omission to exercise any right, power or remedy accruing to either party upon breach or default by either party under this contract, shall impair any such right, power or remedy of either party; nor shall such delay or omission be construed as a waiver of any such breach of default, or any similar breach or default thereafter occurring; nor shall any waiver of single breach or default be deemed a waiver of any subsequent breach or default. All waivers must be in writing.

38. Warranty of Ability to Perform

The Contracting Party warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contracting Party's ability to satisfy its contract obligations. The Contracting Party warrants that neither it nor any affiliate is currently on the convicted vendor list maintained pursuant to Section 287.133 of the Florida Statutes, or on any similar list maintained by any other state or the federal government. The Contracting Party shall immediately notify the Department in writing if its ability to perform is compromised in any manner during the term of the contract.

39. Warranty of Authority

Each person signing the contract warrants that he or she is duly authorized to do so and to bind the respective party to the contract.

IN WITNESS WHEREOF, the FDLE and Contractor have caused this Contract to be executed by their respective undersigned official(s) authorized to do so, effective on the date of final execution.

CutCom Software Inc. d/b/a AppArmor	Florida Department of Law Enforcement
Signature	*Signature*
David Sinkinson	Sonya Avant
Print Name	*Print Name*
Co-Founder	Chief of General Services
Title	*Title*
July 24th 2018	July 31, 2018
Date	*Date*

APPENDIX A - Deliverable Acceptance Form

CONTRACTOR (complete this section)		
Project Title:		
Contract #:		
Date:		
Deliverable Title:		
Deliverable #:		
Deliverable Version (if applicable):		
Phase / Milestone:		
Specify the activities performed to ensure the work can be accepted (e.g. testing, data migration, training)		
CONTRACTOR SIGNATURE		
The Contractor affirms that the deliverable indicated above and delivered to FDLE is complete per the Contract requirements.		
Authorized Signature		
Name (Typed or Printed)		
Title		
Date		
FDLE (complete this section)		
Decision	Accepted	Accepted with Modifications *
*** If Accepted with Modifications indicate date modifications due and any comments**		
Date modifications due:		
Comments:		
Authorized Signature		
Name (Typed or Printed)		
Title		
Date		

APPENDIX B

Project Change Request Form

Change #				
Short Description				
Requested by			**Date**	
Change Type	**Scope**	**Schedule**	**Cost**	**Other**
Contract Amendment Required?	**Yes**	**No**		

Change Description:		
Attachments	**Yes**	**No**

Reason for the Change:
Business Benefits (if applicable):
Implications of Not Making the Change:

Impact of Making Change		
Scope: **Schedule**: **Cost**: **Other**:		
Approve	**Reject**	**Cancel**

<u>Approvals</u>

Contractor Project Manager: ________________________________ **Date:** ________________

FDLE Project Manager: ________________________________ **Date:** ________________

APPENDIX C

AFFIDAVIT OF LIMITED OFFSHORING

Pursuant to Section 23 of the FDLE Standard Terms and Conditions, the undersigned Contractor hereby attests that, with the exception that Contractor is authorized to perform services under the contract from its headquarters in Ontario, Canada, and with the further exception that Contractor may send, transmit, or access State of Florida Data from its headquarters in Ontario, Canada in its performance of this Contract, the Contractor and its Subcontractors do not and will not otherwise perform any of the services under the Contract from outside of the United States, and the Contractor does not and will not otherwise allow any State of Florida data to be sent by any medium, transmitted, or accessed outside of the United States.

Contractor Name: CutCom Software Inc. d/b/a AppArmor

Contractor FEIN #: US TIN: 980494392, Foreign TIN: 857631642

Authorized Signature:

Print Name: David Sinkinson

Title: Co-Founder

Date: July 30th 2018

Sworn to (or affirmed) and subscribed before me on this 30th day of July by Diann Chee, a Notary Public in and for the province of Ontario

(Signature of Notary)

Check One:

□ Personally Known

☒ Produced the following ID Driver's License

Appendix D

Florida Department of Law Enforcement (FDLE)
INFORMATION SYSTEMS SECURITY ADDENDUM

The purpose of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, agency policies and standards.

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of FDLE's information resources are not compromised. Security measures shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all Contractor personnel assigned to FDLE.

1.00 Definitions

1.01 Administration of criminal justice - the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment.

1.02 Agency Coordinator (AC) - a member of FDLE, who manages the agreement between the Contractor and agency.

1.03 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

1.04 Contractor Security Officer (CSO) – an individual designated by the Contractor to administer the Contractor's security program as it pertains to this contract.

1.05 Information Security Manager (ISM) – a member of FDLE, designated by the agency head, to administer FDLE's information security program.

2.00 Responsibilities of FDLE

2.01 FDLE will appoint an AC.

2.02 The AC has the following responsibilities:

a. Understand the communications and records capabilities and needs of the Contractor which is accessing federal and state records through or because of its relationship with FDLE;

b. Participate in related meetings and provide input and comments for system improvement;

c. Receive information and disseminate it to appropriate Contractor employees;

d. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor;

e. Maintain up-to-date records of employees of the Contractor who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable);

f. Train or ensure the training of Contractor personnel. If Contractor personnel access the Florida Crime Information Center (FCIC) System, schedule the operators for testing or a certification exam. Schedule new operators for the certification exam within six (6) months of employment. Schedule certified operators for re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for any other mandated class;

g. The AC will not permit an untrained/untested or non-certified employee of the Contractor to access FDLE information systems;

h. Where appropriate, ensure compliance by the Contractor with Criminal Justice Information System (CJIS) security requirements; and

i. Ensure that Contractor staff undergo background investigations prior to accessing FDLE information systems.

3.00 Responsibilities of the Contractor

3.01 The Contractor shall maintain a security program which meets the requirements of this Security Addendum.

3.02 The Contractor shall assign a Contractor Security Officer (CSO) accountable for the management of this security program. This person shall coordinate with the AC and ISM to establish the Contractor's security program. The Contractor Security Officer for this contract is Christopher Sheppard.

3.03 The Contractor shall ensure that all Contractor personnel assigned to FDLE read this Security Addendum and sign the Certification form attached to this addendum. Signed Certification forms shall be delivered to FDLE's Information Security Manager.

3.04 The Contractor shall establish and maintain a security violation response and reporting procedure to discover, investigate, document, and report on all security violations. Violations which endanger the security or integrity of FDLE information systems or records located therein must be communicated to the AC immediately.

3.05 The Contractor's facilities will be subject to unannounced security inspections performed by FDLE. These facilities are also subject to periodic audits.

3.06 The security plan is subject to annual review by the AC and the Contractor. During this review, efforts will be made to update the program in response to security violations, changes in policies and standards, and/or changes in federal and state law and technology.

3.07 The Contractor and its employees will comply with all federal and state laws, rules, procedures and policies formally adopted by FDLE, Florida's Agency for Enterprise Information Technology, and Federal Bureau of Investigations.

4.00 Site Security

4.01 The Contractor shall dedicate and maintain control of the facilities, or areas of facilities, that support FDLE, when applicable.

4.02 All personal computers and/or terminals physically or logically connected to the computer system accessing FDLE information systems must be segregated and screened against unauthorized use or observation.

5.00 System Integrity

5.01 Only employees of the Contractor and such other persons as may be granted authorization by the AC shall be permitted access to the system.

5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.

5.03 Access to the system shall be available only for official purposes consistent with the appended Agreement. Any dissemination of FDLE data to authorized employees of the Contractor is to be for their official purposes.

5.04 Information contained in or about the system will not be provided to another entity without prior written authorization by the AC.

5.05 All criminal history record information requests must be authorized by the appended Agreement. A current up-to-date log concerning access and dissemination of criminal history record information shall be maintained at all times by the Contractor.

5.06 The Contractor will ensure that its inquiries of FDLE information systems and any subsequent dissemination conform to applicable laws, rules, and policies, as set forth in:

(1) Chapter 817, F.S. Fraudulent Practices
(2) Chapter 119, F.S. Public Records
(3) Chapter 943, F.S. Law Enforcement Act
(4) and this Security Addendum;

5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the criminal justice information system. In no event shall copies of messages or criminal history record information be disseminated other than as envisioned and governed by the appended Agreement.

6.00 Personnel Security

6.01 A background investigation will be conducted on all Contractor employees and the Contractor's vendors which provide system maintenance support.

6.02 The background investigation will conducted by FDLE. This investigation includes an employment check, reference check, credit check, drug screen, and submission of a completed applicant fingerprint card. State and national record checks by fingerprint identification will be conducted for all personnel who manage, operate, develop, access and maintain criminal justice information systems and facilities. Record checks must be completed prior to employment.

6.03 When identification of the applicant with a criminal history has been established by fingerprint comparison, FDLE will review the matter. A Contractor employee found to have a criminal record consisting of any felony convictions or of misdemeanor offenses which demonstrate a pattern of disregard for lawful behavior is disqualified. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

6.04 If an adverse employment determination is made, access will be denied and the Contractor’s Security Officer will be notified in writing of the access denial. This applicant will not be permitted to work on the contract with the FDLE. The Contractor shall be notified of the adverse decision. The Contractor may request FDLE to review an adverse employment decision.

6.05 FDLE’s Security Officer shall maintain a list of personnel who successfully completed the background investigation.

6.06 FDLE will ensure that each Contractor employee receives a copy of the Security Addendum and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of FDLE and available for audit purposes.

6.07 FDLE shall ensure that each Contractor employee authorized to access CJIS network terminals or information provided there from is specially trained in the state and federal laws and rules governing the security and integrity of criminal justice information.

6.08 Visitors to sensitive areas of Contractor facilities must be escorted at all times by a Contractor employee with clearance. Names of all visitors shall be recorded in a visitor log, to include date and time of visit, name of visitor, purpose of visit, name of person visiting, and date and time of departure. The visitor logs shall be maintained for five years following the termination of the contract.

7.00 System Security

7.01 Transmission, processing, and storage of criminal justice information shall be conducted on dedicated systems. Increased reliance should be placed on technical measures to support the ability to identify and account for all activities on a system and to preserve system integrity.

7.02 The system shall include the following technical security measures:

a. unique identification and authentication for all interactive sessions;

b. if warranted by the nature of the contract, advanced authentication techniques in the form of digital signatures and certificates, biometric or encryption for remote communications;

c. security audit capability for interactive sessions and transaction based logging for message-based sessions; this audit shall be enabled at the system and application level;

d. access control mechanisms to enable access to be restricted by object (e.g., data set, volumes, files, records) to include the ability to read, write, or delete the objects;

e. ORI identification and access control restrictions for message based access;

f. system and data integrity controls;

g. access controls on communications devices;

h. confidentiality controls (e.g., partitioned drives, encryption, and object reuse).

7.03 Data encryption shall be required throughout the network passing through a shared public carrier network.

7.04 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

7.05 The Contractor shall establish a procedure for sanitizing all fixed storage media (e.g., disks, drives) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitization procedures include overwriting the media and/or degaussing the media. If media cannot be successfully sanitized it must be returned to the FDLE or destroyed.

8.00 Security Violations

8.01 Consistent with Section 3.05, the Contractor agrees to inform the AC and ISM of system violations. The Contractor further agrees to immediately remove any employee from assignments covered by this contract for security violations pending investigation. Any violation of system discipline or operational policies related to system discipline is grounds for termination, which shall be immediately reported to the AC in writing.

8.02 The ISM will be responsible for reporting security violations to Florida’s Agency for Enterprise Information Technology along actions taken by FDLE and Contractor.

8.03 Security violations can justify termination of the appended agreement.

8.04 Upon notification, FDLE reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including the actual telecommunications link to FDLE information systems.

8.05 FDLE will provide the Contractor with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to FDLE by the Contractor. Upon termination, the Contractor's records containing criminal history record information must be deleted or returned to FDLE.

8.06 FDLE reserves the right to audit the Contractor's operations and procedures at scheduled or unscheduled times. FDLE is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

9.00 Miscellaneous Provisions

9.01 The parties are also subject to applicable federal and state laws and regulations.

9.02 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

9.03 This Security Addendum may only be modified by amendments signed by authorized representatives of FDLE and the Contractor.

9.04 Security-related notices and correspondence shall be forwarded to:

FDLE
Information Technology Services
Attention: Information Security Officer
2331 Phillips Road
Tallahassee, FL 32308

FDLE
INFORMATION SYSTEMS SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I have read and understand the contents of the Security Addendum and the documents referenced therein and agree to be bound by their provisions.

I recognize that information obtained from FDLE information systems should be used only for its intended business purposes and that there is the potential for great harm if misused. I acknowledge that access to FDLE information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of FDLE information systems by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Signature	
Name	
Title	
Company Name	
Date	

FortifyFL Reporting System

This Statement of Work (SOW) describes the Contractor’s and the Florida Department of Law Enforcement (FDLE) responsibilities, requirements, and deliverables for the State of Florida FortifyFL Reporting System. The FDLE and the Contractor shall incorporate the Contractor’s response to the FDLE ITN 1833 via the Best and Final Offer, and Original Technical Reply as applicable throughout this SOW.

SECTION I: Responsibilities

A. Contractor Responsibilities

1. Assign and maintain staff qualified and experienced in operating and maintaining the reporting system.
    a. The Contractor will assure these individuals are available during business hours to address and resolve system and contract issues.
    b. Contractor will maintain an adequate administrative organizational structure to support staff sufficient to discharge its contractual responsibilities as outlined in this agreement.
    c. Contractor is responsible for ensuring its staff providing services under this agreement have the education, experience, and any professional licensure or certification, which may be required by law or the Department to successfully carry out its duties under this contract.
    d. Contractor staff assigned to work on the reporting system may be required to successfully complete an FDLE background investigation.
    e. The Department reserves the right to approve all Contractor and subcontractor project staff. The Department also reserves the right to require a particular Contractor’s or subcontractor’s staff member be replaced on the project, with costs associated with knowledge transfer to be covered under the responsibility of the Contractor.
    f. The Department expects that all nominated Contractor staff listed above will be available for the lifetime of the project under reasonable circumstances. Changes to Contractor project staff listed above will be coordinated through a written Project Change Request approved by the Department’s Executive Management.
    g. Turnover of Contractor staff, including subcontractors, should not obligate the Department to pay additional costs or accommodate schedule delays.
2. Provide project management services.
3. Operate and maintain the reporting system.
4. Identify opportunities for improving business process and workflows.
5. Provide feedback and recommend resolution for testing issues and defects throughout the project.
6. Respond to and resolve documented incidents or problems (including assignment and escalation to third-party contractors).
7. Provide maintenance and support services for the reporting system.
8. Provide monitoring 24 hours per day of the system.

B. FDLE Responsibilities

1. FDLE will assign a Project Manager to serve as the primary point of contact during the planning and implementation of the reporting system.

2. FDLE will provide onsite resources (computer access, telephone, workspace, workstation access, access to key personnel, documentation, data, etc.) to support project activities when/if Contractor is onsite.
3. FDLE personnel will be available to facilitate project activities including, requirements validation, testing, documentation review and inspection of deliverables.
4. FDLE will provide contract management and project closeout support.
5. FDLE's IT Project Management Office will be responsible for project management oversight, with the primary objective of assessing compliance with State of Florida IT project management laws, rules, and policies.

C. Requirements

This section describes FDLE and DLA requirements, technical standards, and expectations for the Anonymous reporting system in which the Contractor is obligated to provide and perform in accordance with the BAFO and Technical Reply (Attachment B).

C.1. Qualifying Requirements

These requirements in Section C.1 must be met by the Contractor.

1	The reporting system is currently in place, fully operational and in use by federal, state or local jurisdictions in the United States.
2	Data center(s) hosting the reporting system are located in the continental United States.
3	The system enables users to submit reports ("tips") through a website and mobile application ("app").

C.2. Functional Requirements

1	System Hosting
1.1	The Contractor must host the reporting system.
1.2	The Contractor is responsible for operating and maintaining the system.
1.3	The banners for the system website and mobile app must be customizable for the State of Florida.
1.4	The system must support both English and Spanish languages.
1.5	The system must be ADA compliant where possible.
1.6	The title for the State of Florida's implementation of the reporting system must be "FortifyFL."
2	Mobile Application
2.1	The Contractor must provide a mobile-application that will enable users to submit tips to the system.
2.2	The mobile app must operate on Android and Apple devices.
2.3	The mobile app must be free of charge to users.
3	Submitting Tips
3.1	A tip must require the user to select a school in Florida. This includes kindergarten through postsecondary, public and charter schools.
3.2	School selection must be from a pick-list based on the geographic location of the user and minimizes the amount of searching required by the user.
3.3	Tips must include other relevant information such as type of tip, priority or alert level, and

	description of behavior or activity.
3.4	Users must have the option to submit tips anonymously or with identifying information.
3.5	Users must have the option to submit attachments with their tip, including images, video, audio, or document files.
3.6	Additional features will be available to the FDLE to improve the functionality of the system.
3.7	The system must send acknowledgement to the user that a tip has been received.
3.8	The system must prompt the user to call 9-1-1 if a tip involves an emergency or immediate threat.
3.9	The system must enable users to securely access tips they have submitted.
3.10	The system must allow users to add information or files to a tip after initial submission.
3.11	The system must provide the ability for users that do not have a mobile device to submit a tip via a website.
4	Routing Tips
4.1	The system must enable state and local administrators to specify the routing of tips.
4.2	The system must provide the ability for state and local administrators to enter contact information.
4.3	The system must route tips to contacts specified by state and local administrators.
4.4	All tips must be concurrently transmitted to FDLE's Office of Statewide Intelligence.
4.5	The system must have the capability to transmit tips to state and local contacts by Email, FAX, message to the system management console, web service, or other similar means.
5	Confirmation of Receipt
5.1	The system must enable specified local agency contacts to confirm receipt of a tip.
5.2	Should receipt of a tip not be confirmed within the time specified during onboarding or as updated by the FDLE anytime thereafter, the system must transmit a second notice to contacts specified by local agency administrators.
5.3	Should receipt of second notice not be confirmed within the time specified during onboarding or as updated by the FDLE anytime thereafter, the Contractor should confirm receipt by initiating a telephone call (or other mechanism as agreed by the Contractor and the FDLE) the specified local agency contact(s).
6	Update Status
6.1	The system must provide agencies with the ability update status of a tip.
6.2	The system must provide agencies with the ability to enter case numbers.
7	Record Maintenance
7.1	The system must maintain audit logs of events associated with tips, including receipt, routing, confirmation, and status update.
7.2	Ownership of tips and associated files must reside with the State of Florida.
7.3	Tips and associated files must be maintained in the system per the Florida Public records requirements.
7.4	Upon termination of the contract, the Contractor shall deliver to FDLE an electronic copy of all tips and associated files in a manner specified by FDLE.
7.5	Following FDLE's confirmation of receipt of the electronic copy, the Contractor shall destroy all records of tips and associated files. Following destruction of these records, the Contractor shall deliver written certification to FDLE that all records have been destroyed.
8	Management Console / Dashboard

8.1	The system must provide a management console / dashboard for use by state and local agency administrators.
8.2	The management console / dashboard must provide functions described below.
8.2.1	Create, update, and delete contact information.
8.2.2	Specify routing of tips within a county and agency.
8.2.3	Export individual tips and attached files.
8.2.4	Perform basic searches.
8.2.5	Perform complex searches (such as Boolean and fuzzy string searching).
8.2.6	Run reports.
8.2.7	Extract files.

C.3. Technical (Non-Functional) Requirements

1	Project Management
1.1	While FDLE assumes primary responsibility for preparing project management documentation, the Contractor must work with FDLE to produce and maintain project management documentation in accordance with FDLE's IT Project Management Standards.
1.1.1	Project Plan. The vendor must provide a project plan for the implementation and a phased rollout of the system. The project plan must include the elements shown below. • Project Approach o Description of Major Phases and Activities required to complete the project o Staff assigned to the project and their roles o Description of how the project will be managed o Tools required to complete the project • Project Schedule in Teamwork project management software including the following components o Tasks/Activity Definition o Major Milestones o Dependencies(predecessors & successors) o Staff Assignments to Tasks o Estimated Activity Durations (in hours) o Start & End Dates for Activities
1.2	The Contractor is responsible for coordinating Requirements Validation and producing a Requirements Validation Document. The Requirements Validation Document must include at a minimum, but not be limited to the following: • Workshops • Assessments • Business Process Analysis
1.3	The Contractor must assist FDLE in producing and maintaining a Requirements Traceability Matrix.
1.4	The Contractor must prepare an Implementation Plan.
1.5	The Contractor must take part in weekly status meetings during implementation of the system.
2	Security
2.1	To the maximum extent practical, Contractor will conform to Rule 74-2, Florida

	Administrative Code (Florida Cybersecurity Standards). Contractor may find it necessary to employ compensating security controls when they are unable to implement a specific security standard or the standard is not cost-effective due to the specific nature of a system or its environment. The Contractor may, with FDLE's documented approval, employ compensating control(s) if they document their analysis and the risk associated with employing the compensating control.
2.2	Contractor must ensure that policies and procedures for securing Florida information and system resources are in place and understood by all affected parties.
2.3	Contractor must ensure that security controls are in place to minimize risks to the confidentiality, integrity, and availability of the system and data.
2.4	The system must be compliant with HIPAA and FERPA.
2.5	All data must be encrypted in transit using TLS 1.2 or higher, with minimum cypher strength of 128 bits (AES 256 preferred).
2.6	Access to information in the system must be based on user roles and associated access rights. Access should be assigned on the principle of "Least Privilege" and managed according to documented procedures.
2.7	System resources must be protected by physical controls. Contractor must maintain procedures to manage physical access to information technology facilities housing Florida information.
2.8	Contractor must implement procedures to protect Florida information from loss, destruction, and unauthorized or improper disclosure or modification.
2.9	Logical controls must be in place to segregate and protect Florida's information.
2.10	Contractor must notify FDLE of any suspected cybersecurity incident or breach of Florida information within 24 hours of discovery.
2.11	The identity of the reporting party received through the app and held by the department, law enforcement agencies, or school officials is confidential and exempt from s. 119.07(1), FS, and section 24(a), Article I of the State Constitution. Any other information received through the app and held by the department, law enforcement agencies, or school officials is exempt from section 119.07(1), F.S, and section 24(a), Article I of the State Constitution. [Per SB 1940/Chapter 2018-001, Laws of Florida]
3	System Support
3.1	The system must be designed and developed to support a 24/7 production environment and reporting system.
3.2	Contractor must ensure that software products used in the system (e.g., operating systems, web server platforms, database management, development frameworks) are upgraded or replaced prior to reaching end-of-life or unsupported status.
3.3	The Contractor will provide the Premium Support Plan (Help Desk) that is available during FDLE business hours (Monday – Friday, 8:00 a.m. – 6:00 p.m. Eastern Time) to assist with usability questions, problem analysis and for reports of technical issues.
3.4	The Contractor must have a defined escalation plan for technical problems that cannot be resolved by the Help Desk. The escalation plan must include a definition of severity levels and specific escalation procedures based upon the severity of the technical problem.
3.5	The Contractor agrees to share with FDLE their road map for future development and enhancements of the system.
4	Service Level Agreement
4.1	System Availability:

	Minimum of 99.5% uptime, 24 hours a day, 7 days a week, and 365 days a year.
4.2	System Recovery Time Objective (RTO) – One (1) hour
4.3	System Recovery Point Objective (RPO) – Thirty (30) minutes
4.4	Incident Severity Levels and Response Times must be provided in accordance with the Contractor's escalation plan:
	Business Critical – Maximum response time one (1) hour
	Degraded Service – Maximum response time four (4) hours
	General Issue – Maximum response time one (1) business day
4.5	The Contractor must notify FDLE at least two (2) work days prior to planned system downtime. FDLE will specify the contacts and method of notification.
4.6	All major changes to the system, such as scheduled maintenance, must be announced to FDLE (2) work days prior to planned implementation and should be applied during non-peak hours (8 PM to 7 AM ET).

C.4. Public Awareness and Training Requirements

1	Public Awareness and Training
1.1	The Contractor will provide a Public Awareness and Training Plan.
1.2	The Contractor will provide training services regarding use of the system to school staff, administrators and law enforcement personnel.
1.3	The Contractor will provide public awareness services and materials to schools.
1.4	The Contractor will work with the State in the development and delivery of the training and awareness programs.
1.5	The Contract will produce and deliver written and online/webinar trainings and training materials for school staff, administrators and law enforcement personnel.

D. Deliverables

This section defines the Contractor Deliverable requirements within each identified Deliverable post Contract award. Contractors are to confirm their understanding and acceptance of the Deliverable as identified within this Section.

Project deliverables will be measurable, verifiable, and quantifiable to enable FDLE to determine that progress has been made, and provides evidence of progress corresponds with the payment requested.

Deliverable I: Requirements Validation Document (RVD) and Project Plan

Deliverable I will define and document the anonymous reporting system processes, workflows, and requirements to identify any gaps between the baseline software version and the Department's end-product requirements.

Deliverable I will consist of the following activities:

Scope and Plan: This initial Deliverable will include an in-person kick off meeting with the Contractor and the Department primary points of contact at an agreed upon location to complete the following:

- define roles and responsibilities for all parties;
- establish general scope and magnitude;
- initial organization and planning;
- define current assumptions.

Workshops: The Contractor and the Department will jointly establish interactive meetings or sessions by functional business area for the purposes described below on the topic areas described in the Functional Requirements.

- clarify common terminology;
- identify, review, and establish requirements;
- identify, review, and establish design decisions;
- identify, review, and establish plans to implement workflows;
- identify, review, and establish user and administrative roles, responsibilities, permissions, and keys;
- identify, review, and establish a messaging and communication component for providing tips, messages, and notifications to internal and external users, and system administrators;
- identify and establish forms, which must include, but are not limited to elements required in the functional requirements section.

Deliverable 1: Requirements Validation Document (RVD) and Project Plan The Contractor will develop and deliver a requirements document as described in Deliverable 1, System Definition and Design.	
Minimum performance criteria:	Performance will be the completion of activities identified in the System Definition and Design as required to produce the deliverable. Workshops will be conducted in accordance with scope of work that includes, at a minimum, the elements described in the Functional Requirements.
Documentation:	A final requirements document and Project Plan accepted in writing by the Department.

Deliverable 2: Pilot Group Testing and Development Deployment The Contractor will provide, implement, and deploy fully functional user application in the designated Development environment available for Pilot Group testing.	
Minimum performance criteria:	Performance will be implementation, and deployment of functional software subscription.
Documentation:	Written acceptance of the licenses in a development environment by the Department

Deliverable 3: Administrator Training The Contractor will provide and deliver written and online/webinar trainings and training material for the anonymous reporting system in accordance with agreed upon curriculum and training schedules.	
Minimum performance criteria:	Contractor will conduct comprehensive train-the-trainer sessions for a minimum of *TBD* State personnel on the anonymous reporting system as described: a. Classroom or computer-based lab setting b. Training will be focused on a minimum of the following topic areas: • Leading Application Users • Application System Administrators • Technical Operations and Administration Staff Contractor will author and produce comprehensive written and online training curriculum as agreed upon in collaboration with the Department.

	Contractor will provide a digital and hard copy production of the following training materials for the Department and each training participant: a. User's Guide with corresponding online help guide for general users b. Administrator's Guide for application administrators
Documentation:	Digital and hard copy presentations, curriculum, agendas, or other work products as described, and delivered by the Contractor and accepted in writing by the Department.

<u>Deliverable 4: Production Deployment</u>

The CONTRACTOR will work with the Department to ensure the system meets 100% of the requirements defined in Deliverable I: System Definition and Design. This Deliverable will result in the Department verifying and accepting the system, and deploying the system into production.

Deliverable 4 will consist of the following activities:

<u>User Acceptance</u>: The Department will verify system operations and ensure compliance with requirements defined in Deliverable I: System Definition and Design. The Department and CONTRACTOR will complete Deliverable 2: Pilot Testing and Deployment. <u>Installation</u>: The CONTRACTOR will deploy Anonymous Reporting System in the designated vendor-hosted production environment and ensure successful operations.

Deliverable 4: Production Deployment The Anonymous Reporting System will be deemed complete when the Contractor corrects all tickets and issues categorized as 4 or 5, and the Department verifies the subscription meets 100% of the requirements defined in the RVD. Change Controls should be documented by the Contractor with FDLE Program Manager approval for any deviations.	
Minimum performance criteria:	Performance will be the completion of activities identified in Deliverable 4 as required to produce the deliverable.
Documentation:	A final requirements document accepted in writing by the Department

Deliverable 5: System Acceptance System Acceptance will occur when all project tasks have been completed. This includes all documentation, project management and administrative takes and resolution of severity Level 3, 4, and 5 defects.	
Minimum Performance Criteria:	No Open Severity Level 3, 4 or 5 Defects. All project documentation updated. All deliverables accepted.
Documentation:	Project lessons learned meeting held and documented

D. <u>Performance Standards and Financial Consequences</u>

Section 287.058 (1)(h) Florida Statutes, requires the Department to specify financial consequences if the Contractor fails to perform in accordance with a Contract. The financial consequences for failure to comply with this Contract are set forth in the following Table:

Performance Standards and Financial Consequences	
Performance Standard	Financial Consequences
Implementation deliverables are fixed rate as described in the Statement of Work (SOW). Upon successful completion of activities described in each deliverable, payment(s) will be processed and approved upon written acceptance of work product(s) by the FDLE ITS Project Manager.	If the Contracting Party fails to meet the minimum level of service or performance identified in this Contract, or is customary for the industry, then the Department will apply financial consequences. Financial consequences may include but are not limited to withholding payments until the deficiency is cured, withholding one and one-half percent (1.5%) of the Deliverable fee specified in the Contract for each day that the deliverable is late, imposition of other financial consequences and termination of contract and requisition of goods or services from an alternate source. Any payment made in reliance on Contracting Party's evidence of performance, which evidence is subsequently determined to be erroneous, will be immediately due to the Department as an overpayment.

SECTION II: DELIVERABLE ACCEPTANCE PROCESS

The deliverables required in Section II: Scope of Work will be reviewed and accepted by the Department in writing in order to process payments. The Department supports a preliminary review process. To facilitate the acceptance of a final deliverable for payment, the preliminary review allows the Contractor to submit the deliverable for initial review. The Department will at its earliest opportunity review deliverables for compliance with the contract requirements, using the following process:

Preliminary Review: The Contractor may provide each deliverable to the FDLE Project Sponsor and FDLE Project Manager for preliminary review. The Department will determine the individuals who will review the deliverable during the review, and will provide comments regarding the state of the deliverable and any issues or concerns needing to be addressed by the Contractor. The preliminary review is an informal review of the deliverables and is not considered part of the final review. The final review will begin when the Contractor submits the deliverable using the documentation and procedures outlined in the next section.

Final Review and Acceptance of Deliverables: The Contractor should notify FDLE Project Sponsor and Project Manager in writing, using the Deliverable Acceptance Form specified in Appendix #, when a deliverable is ready for final inspection. Deliverables will be submitted in accordance with the due date on the Project Schedule.

The FDLE Project Sponsor, FDLE Project Manager, and any Subject Matter Experts (SMEs) identified by the Department will complete a full review and inspection of the deliverable as soon as practical, and identify defects associated with the deliverables (if any). The FDLE Project Sponsor and Project Manager will document defects and assign a severity level using the criteria described in the table below and deliver this documentation to the Contractor.

SEVERITY	CLASSIFICATION	CRITERIA
5	**Critical**	Highest Risk Level - Occurs when the system is not functioning and there is no work-around - Total system failure - Catastrophic failure
4	**High**	Impairment of critical system functions or processes – no workaround or solution exists – High Risk of Failure
3	**Moderate**	Impairment of system functions or processes – a documented workaround exists – Medium Risk
2	**Low**	Non-Critical Failure – Occurs when a system component is not functioning, but the system is still useable for its intended purpose, or there is a reasonable work-around. – Little impact – Low Risk
1	**Inconvenience**	Inconvenience – Occurs when system causes a minor disruption in the way tasks are performed but does not stop workflow – User is able to tolerate inconvenience - No Risk

A formal approval, documented through a deliverable acceptance form signed by Contractor, FDLE Project Sponsor, and FDLE Project Manager must be completed as described above. The decision by the Department will be either “Accepted,” “Accepted with Modifications,” or “Rejected.”

If the decision is “**Accepted**,” the Contractor will be notified and the FDLE Project Manager or Contract Manager will send a completed Deliverable Acceptance Form for the deliverable(s) to the Contractor.

If the decision is “**Accepted with Modifications**,” the Contractor will be notified, but will be required to address the issues or defects raised in a timeframe specified by the FDLE Project Sponsor and FDLE Project Manager on the Deliverable Acceptance Form. The Contractor and Department will discuss the defects and develop a mutually agreed plan for correcting the defects. Defects assigned a severity level of 3, 4 or 5 must be corrected in order for the Department to accept a deliverable. Once modifications have been incorporated and reviewed by the FDLE Project Sponsor and FDLE Project Manager, the Contractor will submit a second Deliverable Acceptance Form for signature which documents that the modifications have been made to the deliverable.

If the decision is “**Rejected**,” the Contractor will be required to address the deficiencies noted on the response in a timeframe agreed upon by the Department and the Contractor and follow the submission, review, and acceptance process.

Deliverables must be “Accepted” or “Accepted with Modifications” in order to authorize payment of the deliverable, if applicable. The submission of a completed Deliverable Acceptance Form to the Contractor will initiate invoice for payment of that deliverable to the Department.

A second or subsequent signed Deliverable Acceptance Form with a decision of “Accepted” or “Accepted with Modifications” previously accepted with modifications will not authorize a payment. A Deliverable Acceptance Form with a decision of “Rejected” will not authorize a payment for the deliverable.

Financial consequences associated with performance failure are included in Section II: Scope of Work. However, if service/deliverable issues continue to be documented by the Department one-hundred and twenty (120) calendar days after the deliverable due date, then the Department, at its sole discretion, may:

- terminate the contract;
- extend the acceptance period; or
- accept the service(s)/deliverable(s) at their current level of performance and at a negotiated price commensurate with that level of performance.

If the Department accepts the system/product at its then current level of performance, the Department may submit to the Contractor an equitable adjustment to the cost of the system. The Contractor may accept or reject the adjusted cost submitted by the Department. In the event the Contractor rejects the Department's adjusted cost, the contract should be terminated and the Department should be liable for no additional charges.

Acceptance of a Prepared Software Deliverable (either configured or customized for the Department) after Acceptance Testing but before the deliverable has been put into production (Interim Acceptance)

Interim Acceptance should not preclude the Department from subsequently identifying deficiencies and declining to provide Final Acceptance on that basis. Further, prior Interim or Final Acceptance of a deliverable should not preclude the Department from also declining to accept a subsequent deliverable that does not operate properly due to defects in the prior accepted deliverable. Final acceptance (i.e. for payment purposes) should be considered to occur when each deliverable has been operating in production without any material deficiency for 60 calendar days of full production with all functionality.

All written deliverables will be provided in the following electronic formats:

- Microsoft Word for text
- Microsoft Excel for spreadsheets
- Microsoft Project for schedules
- Microsoft PowerPoint for presentations
- Microsoft Visio for diagrams

SECTION III: ISSUE MANAGEMENT

In the event that disputes or performance issues arise, the FDLE Project Manager will document and deliver the specific issue(s) to the Contractor Project Manager. The Contractor will be given the opportunity to address and resolve the issue(s) within a reasonable period of time. Issues associated with FDLE's performance under this agreement will be documented by the Contractor and delivered to the FDLE Project Manager. The FDLE will be given the opportunity to address and resolve the issue(s) within a reasonable of period of time.

Issues will be documented in an Issues Log which will be maintained by Contractor Project Manager. If a dispute or issue(s) is not resolved between the FDLE Project Manager and the Contractor Project Manager, the dispute(s) or issue(s) may be escalated through the escalation levels provided in the table below.

ISSUE ESCALATION

Level	FDLE	Contractor
1	Project Manager	Project Manager
2	Chief Information Officer	Executive Manager
3	Assistant Commissioner	Senior Corporate Executive

Contractor will notify the Department's contract manager and FortifyFL Project Manager in writing a minimum of one (1) week prior to making changes in location or contact information that will impede the Department's ability to contact the Contractor.

SECTION IV: SCHEDULE

The Contractor and FDLE will work together to produce a project schedule. Teamwork project management software will be used as the scheduling tool. A preliminary schedule will be prepared at the beginning of Deliverable 1. Major milestone date to be included in the schedule:

A more detailed, elaborated schedule will be produced at the end of Deliverable 1. After the elaborated schedule is approved by the Contractor and FDLE, the project baseline schedule will be set.

FDLE will be responsible for maintaining the baselined project schedule.

SECTION VI: ADMINISTRATION

Changes to the following points of contact and chief officials below must be submitted to the Department pursuant to the Change Management process, Section 3 of FDLE Contract.

The following Contractor staff is designated for this contract:

Executive Manager / Chief Official	
Name	David Sinkinson
Title	Co-Founder
Address	PO Box 12 Station A Toronto ON M5W1A2
Phone	416-708-4688
Email	dsinkinson@apparmor.com

Program / Project Manager	
Name	Chris Sinkinson
Title	CTO and Co-Founder
Address	PO Box 12 Station A Toronto ON M5W1A2
Phone	647-992-7919
Email	csinkinson@apparmor.com

Lead Engineer	
Name	Chris Sinkinson
Title	CTO and Co-Founder
Address	PO Box 12 Station A Toronto ON M5W1A2
Phone	647-992-7919
Email	csinkinson@apparmor.com

Contract Administration and Financial Point of Contact	
Name	David Sinkinson
Title	Co-Founder
Address	PO Box 12 Station A Toronto ON M5W1A2
Phone	416-708-4688
Email	dsinkinson@apparmor.com

The following FDLE staff is designated for this contract:

Project Sponsor	
Name	Joey Hornsby
Title	Chief Information Officer
Phone	850-410-8455
Email	joeyhornsby@fdle.state.fl.us

Project Manager	
Name	Cheryl Gilman
Title	Planning Consultant
Phone	850-410-8505
Email	cherylgilman@fdle.state.fl.us

Contract Manager	
Name	Angela Githens
Title	Government Analyst II
Phone	850-410-7715
Email	angelagithens@fdle.state.fl.us

AppArmor Best and Final Offer (BAFO) – ITN 1833 Fortify FL

VIA Email
June 25th 2018

FDLE
Attention: Sonya Avant
Procurement Officer
PO Box 1489,
Tallahassee, Florida, USA 32302-1489

Dear Sonya and the FDLE decision Committee,

Thank you for the opportunity to present our solution to you on June 20th. We are thrilled to have the opportunity to offer you a Best and Final Offer (BAFO) for ITN 1833 "FortifyFL". Per your letter of June 22nd, we have addressed all items in order and provided an updated Attachment J at the end of this letter. If there are any questions, please direct them to me, David Sinkinson, at dsinkinson@apparmor.com

1. Listing of Additional Features included in proposed price reply

Included in our BAFO are the following app and dashboard features:
(a) Advanced Incident Reporting with Automatic Routing and primary and secondary "alerting" notifications including:

   i. Email Notifications
   ii. Push Notifications
   iii. SMS Notifications
   iv. Outbound Calling
   v. Faxing
   vi. Dashboard notifications
   vii. Web based notifications (RSS, CAP, etc)

(b) Emergency calling capability;
(c) Push notification capability (unlimited usage);
(d) Mobile "BlueLight" (panic button) emergency button with location share;
(e) Friend Walk location sharing with a contact;
(f) Virtual walk-home location sharing with a dispatcher in the cloud dashboard;
(g) Embedded information for additional FDLE, Community or other services as required;
(h) Mapping capabilities including but not limited to a crime map;
(i) Unlimited "Geofencing" capabilities;
(j) Additional Administrative dashboards as required; and
(k) Emergency plan documentation;
(l) Unlimited Usage of Content Management System

2. Additional Features not included in the price reply

Mobile App Features:

(a) WorkAlone Premium Feature: A capability which, when enabled, can have the app automatically check in on a user who has indicated that they're "working alone" and can even automatically trigger a distress call to a contact in the individual's phone or emergency services. A video is available here: http://video.apparmor.com/workalone/.

Pricing for this feature is an additional $10,000 annually.

(b) CheckIn Premium Feature: A capability which, when enabled, enables administrative users to initiate a "CheckIn" to the entire list of users or a targeted subset of the user base. Most commonly a subset is targeted to reflect the nature of the crisis (for instance, a threat in a particular county would trigger a "CheckIn" to users in that county). A video is available here: http://video.apparmor.com/checkin/

Pricing for this feature is an additional $10,000 annually.

Mass notification mechanisms, other than push notifications, for use outside of reporting system are also subject to additional pricing. They have been briefly described and listed below:

(a) Emergency[1] SMS Messaging: The ability to send out mass text messages with the intended throughput to meet all targeted users in 1-5 minutes.

Cost for this capability: $35,000 annually. Note that there is also a per message cost of $.05 (5 cents) per message sent. This amount is subject to change if telecommunications firms increase the per message rate which is payable by AppArmor.

(b) Unlimited Email Messaging: The ability to send out mass email messages with the intended throughput to meet all targeted users in 1-5 minutes.

Cost for this capability: $15,000 annually. No per usage fee.

(c) Emergency Outbound Calling: The ability to send out mass outbound calls with the intended throughput to meet all targeted users in 1-5 minutes.

Cost for this capability: $25,000 annually. Note that there is also a per message cost of $.05 (5 cents) per message sent. This amount is subject to change if telecommunications firms increase the per message rate which is payable by AppArmor.

[1] Emergency Messaging is defined as a message issued to alert the campus/organization of a confirmed, active situation that poses an immediate threat to life, safety, and security and/or property in the following scenarios: active shooter, bomb threat, evacuation, fire alerts, suspicious package, inclement weather, hazardous material alerts, utilities outages, medical assistance.

(d) Desktop Notifications (with optional "panic" button): The ability to screen lock PC and MacIntosh Corporate devices and provided an optional "soft panic button" via the system tray. Intended throughput to meet all targeted users in 1-5 minutes.

Cost for this capability: $2.50 annually per registered device. No per usage fee.

(e) Social Media Broadcasting: The ability to broadcast to multiple Twitter and Facebook handles with the intended throughput to meet all targeted users in 1 minute.

Cost for this capability: $1,500 per Twitter Handle and/or Facebook page. No per usage fee.

(f) RSS Feeds: The ability to broadcast an RSS/ATOM/XML feed with the intended throughput to meet all targeted endpoints in 1-5 seconds.

Cost for this capability: $5,000 annually. No per usage fee or limit on feeds.

(g) HTTP Activation: The ability to broadcast an alert to organizational websites with the intended throughput to meet all targeted endpoints in 1-5 seconds.

Cost for this capability: $10,000 annually. No per usage fee or limit on sites activated.

All of the above services and directly administered and aggregated in the AppArmor Cloud Dashboard. Additional volume discounts may apply if the state determines to apply these services in a large deployment. Updated pricing would be determined in negotiation.

I can confirm that these additional features may be available to the State at any time during the initial implementation phase, or any time during the base contract term or renewal year options, with final pricing subject to negotiation if implemented.

3. New Features

I can confirm that any new features that may be developed in the future by AppArmor may be made available to the State at any time during the base contract term or renewal year options, with final pricing subject to negotiation if implemented.

4. Support Level

I can confirm that the Premium Support Level Agreement (SLA) is included in the proposed price reply.

5. Advanced Searching

As was briefly demoed and discussed, I can confirm that AppArmor can provide advanced features, including partial word and wildcard search capability for search results. AppArmor will add additional capabilities to the search mechanisms as required by the FDLE.

6. Additional Search Fields

As was briefly discussed, AppArmor can easily add additional fields to both the tip submission from an end user and in the administrative console for searching purposes. These fields can be added and removed in real-time by FDLE. This will be configured to the satisfaction of FDLE.

7. Implementation Schedule Update

An updated timeline has been included below.

Milestone	Anticipated Time Requirement	Notes
Award of RFP	n/a	FDLE's proposed announcement of successful vendor
"Kickoff" Meeting	30 minutes	Ideally, we'd have the kickoff call as soon as possible after being notified of award. This call would include the FDLE project manager and simply "set the table" for the next steps.
Group Webinar on IT and AppStore Objectives	60-90 minutes	We envision a second call with all FDLE stakeholders (IT, Ops, Marketing) where we coordinate on next steps for AppStore, content & branding, and feature objectives.
Group Webinar on Content Objectives		
Group Webinar on Aesthetic Objectives		
App Blueprints complete by FDLE. To be mirrored on webpage.	5-10 Business Days	FDLE will have been directed (see more details in subsequent pages) to complete an app "blueprint". These will be provided to AppArmor on the 10th with the intention of building version 1 of the app by the 13th of July. FDLE will confirm initial app content at this time, including reporting form fields.
App Version 1 of content ready	3 Business Days	Content in the apps is ready for staff to test. Fulfilled by AppArmor
Geofences and Institution List added to AppArmor Systems. Institutional Contacts uploaded as well	15 Business Days	Institutional contacts for the State and FDLE contacts added to system. Institutions added as well. Geofences built.

App "Graphics" finished and loaded. Website Aesthetics ready.	3 Business Days	Hard coded graphics, app name, and other related branding elements are complete and loaded in the app. Note: Have been created already by FL students
Mobile App Pre-Deployment Testing Complete	5 Business Days	Testing will be conducted over a week-long period to ensure all components are functioning as intended.
AppStore and Google Play Invitations sent to AppArmor deployment team. Website in production but password protected.	3 Business Days	The appropriate staff at the FDLE will invite the AppArmor team to the AppStore and Google Play accounts for the institution for the purposes of submitting the apps to the appstores.
Mobile App Submissions and Deployments Complete. Apps live, site live.	4 Business Days	Throughout the first week of August, AppArmor will deploy app to the appropriate AppStores.
Production Testing of all Features Notifications	5 Business Days	Production testing – App is "live", site is public. Gap analysis conducted and suggested changes implemented.
Training of Staff	1-5 Business Days	Once the app and site have been deployed successfully, we believe this is the ideal opportunity to begin training. NOTE: Training may be automated on a dashboard level.
Shift from Onboarding to Support	N/a	The implementation is complete and the State will take full control of the system. An AppArmor account manager is allocated for ongoing support

Note that this plan will be formalized on the kickoff call. Our Teamwork software will be deployed at this time, meaning that the plan will also be easily accessible by FDLE.

8.Conflicting Legal Agreement Clauses

AppArmor confirms that any terms which conflict with Florida Law, or the FDLE ITN Terms and Conditions are subject to modification. In particular, we are aware that FDLE Terms and Conditions will prevail.

9. Attachment J

Included on the next page. We have provided a 10% discount on the one-time fee to demonstrate our eagerness to work with FDLE on this exciting project.

Thank you for the opportunity to earn your business!

Date: June 25th 2018

David Sinkinson
Co-Founder,
AppArmor
416-708-4688
dsinkinson@apparmor.com

Prices identified in this section are for the implementation of the FortifyFL System.

Deliverable	Description
1	**Requirements Validation Document (RVD) and Project Plan**
2	**Pilot Group Testing and Development Deployment**
3	**Administrator Training**
4	**Production Deployment**
5	**System Acceptance**
TOTAL PRICE FOR SYSTEM IMPLEMENTATION	**$** 82,800

Annual Subscription / License Fee	Annual Price
1st Year Contract	$ 57,200
2nd Year Contract	$ 57,200
3rd Year Contract	$ 57,200

Annual Subscription / License Fee Contract Renewals	Annual Price
1st Year Contract Renewal	$ 46,400
2nd Year Contract Renewal	$ 46,400
3rd Year Contract Renewal	$ 46,400

TOTAL GRAND PRICE TO INCLUDE: **IMPLEMENTATION, ANNUAL SUBSCRIPTION / LICENSE FEE, AND CONTRACT RENEWAL OPTIONS.**	**$** 393,600

Signature	
Respondent Company Name	CutCom Software Inc. (Alias: AppArmor)
Federal Tax ID Number	Canadian Corporation: DUNS - 202593836, US TIN: 98-0494392, Foreign TIN: 857631642
Respondent Physical Address	545 King Street West
City, State, Zip	Toronto Ontario Canada M5W 1A2
Primary Contact Name / Title	David Sinkinson, Co-Founder
Phone Number	4167084688
Email Address	dsinkinson@apparmor.com

AppArmor

THE INDUSTRY STANDARD IN CUSTOM REPORTING APPS

FORTIFY FL REPORTING SYSTEM

Invitation to Negotiate

Florida Department of Law Enforcement

FDLE-ITN-1833

AppArmor

1 – SYSTEM HOSTING

1.1 – The Contractor should host the reporting system.

The AppArmor platform is entirely hosted on AppArmor systems. The platform is a user friendly, cloud based dashboard that houses the reporting capabilities, a content management system for the mobile app (see description in Tab 6), mass notification capability (also in Tab 6), and dispatcher-based services. It is accessible 24/7 anywhere in the world (assuming that the user has account credentials). The State and FDLE are able to have unlimited dashboard accounts on our platform.

The administrative dashboard provides reporting options for non-technical administrators, such as: number of downloads, push notification subscribers, incidents reported (among other information), previous mass notifications, and more. Regular reports can be automatically generated for the purposes of informing key FDLE personnel. Additional reporting can be added upon request.

For authentication, AppArmor supports SAML V2.0 the standard Browser SSO profile and can rely on platform browser to handle authentication to allow for integration via the standard profile. AppArmor has integrated at many other organizations' various forms of single sign on support. For FDLE we would accommodate this request if desired.

See "Tab 6" for a description of the administrative content management system as well as other important app capabilities which will add more value for the State and FDLE.

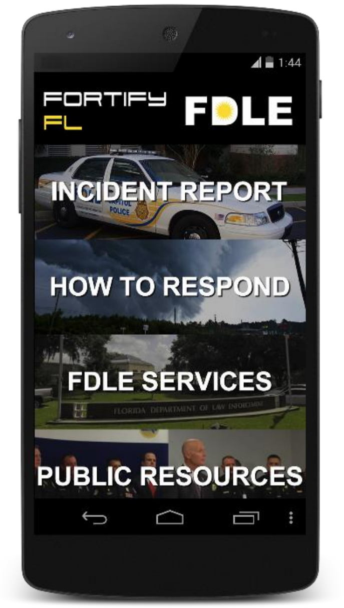
1.2 - The Contractor is responsible for operating and maintaining the system.

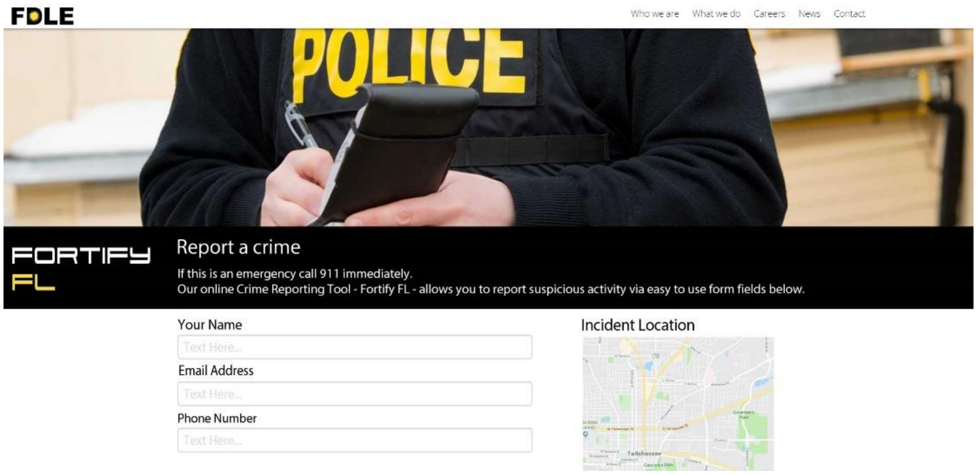
AppArmor is wholly responsible for the operation and maintenance of the system. Updates are provided to the system in such a way that allows for zero upgrade/maintenance downtime; we use a DevOps "Continuous Delivery" Approach to ensure the software for the mobile app and dashboard are up to date.

Further, AppArmor has a dedicated global support team which would assist with all end-user issues. More details are provided on this in Tab 4, Section 3.

1.3 - The banners for the system website and mobile app should be customizable for the State of Florida.

AppArmor is an entirely "white labelled" product. This means that whether the organizations is deploying a mobile app, reporting webpage, mass notification system, or other AppArmor product, it is always entirely branded to the partner organization. To further emphasize this point, we've included some concept art below which identifies what we believe a FortifyFL app and webpage could resemble. Note that of course, all graphics and visual identity will be determined in close collaboration with the State. They are modifiable at any time.





Report a crime

If this is an emergency call 911 immediately.
Our online Crime Reporting Tool - Fortify FL - allows you to report suspicious activity via easy to use form fields below.

Your Name
Text Here...
Email Address
Text Here...
Phone Number
Text Here...

Incident Location

1.4 - The system should support both English and Spanish languages.

The AppArmor system is multi-lingual, and can fully support English and Spanish Languages from an end-user reporting perspective. For the purposes of this ITN, we would ensure that the languages are accurately displayed in parity in English in Spanish in coordination with experts at the State.

Currently the dashboard interface, which is in this context would only face internal stakeholders, is only available in English. While reports from Spanish speaking users would be in Spanish, the interface ingesting these messages would be in English. If necessary and in coordination with the State, AppArmor could have the dashboard translated to include the Spanish language.

1.5 - The system should be ADA compliant where possible.

AppArmor is ADA compliant. Our apps are regularly audited by organizations to vet our compliance with the accessibility mode of the smartphones and the browsers (for the online dashboard). We are happy to provide this documentation upon request. We are also happy to provide a VPAT upon request.

The mobile app solution is also fully compliant with “Accessibility Mode” on the devices, meaning that it meets all of the required regulations per appropriate law. This includes font size increases, text to speech and more. The dashboard includes all of the required accessibility options for web browser as identified in the Web Content Accessibility Guidelines (WCAG).

AppArmor is fully committed to the accessibility of the platform and is willing to make improvements should any shortcomings be discovered. As an example of this commitment, we deployed an app at the Rochester Institute of Technology. On their campus is the National Technical Institute for the Deaf. Consequently, numerous members of the community requested a series of features to make the app friendlier, outside of accessibility mode, from an accessibility perspective. We then built a new feature – a reporting button feature that only uses a text message – in a one-week timeframe to meet the needs of the community.

1.6 - The title for the State of Florida's implementation of the reporting system will be "FortifyFL."

Absolutely. The State and FDLE may call the reporting system by any name and even change it in the future should there be a need to do so.

2 - MOBILE APPLICATION

2.1 - The Contractor should provide a mobile-application that will enable users to submit tips to the system.

AppArmor is the industry standard in custom mobile safety and reporting apps. We've deployed mobile apps for over 170 organizations on iOS and Android (previously Blackberry as well). Our apps are always branded to the organization and include over 50 powerful safety features including advanced mobile reporting capabilities.

2.2 - The mobile app should operate on Android and Apple devices.

The mobile solution is supported on iOS and Android in parity, meaning that they are exactly the same on both platforms, simplifying education efforts and support. Further, we support over 10,000 iOS and Android smartphones and tablets.

2.3 - The mobile app should be free of charge to users.

Yes. The app is always free to end users. The app is also submitted under the appstore account of the State – this means that technically speaking, the State is setting the price. Note: this is an important distinction of the AppArmor platform; by submitting the app under the AppStore and Google Play account of the State, this provides the state with more control over user information and ultimately business flexibility should it wish to "switch" to another vendor in future years.

3 - SUBMITTING TIPS

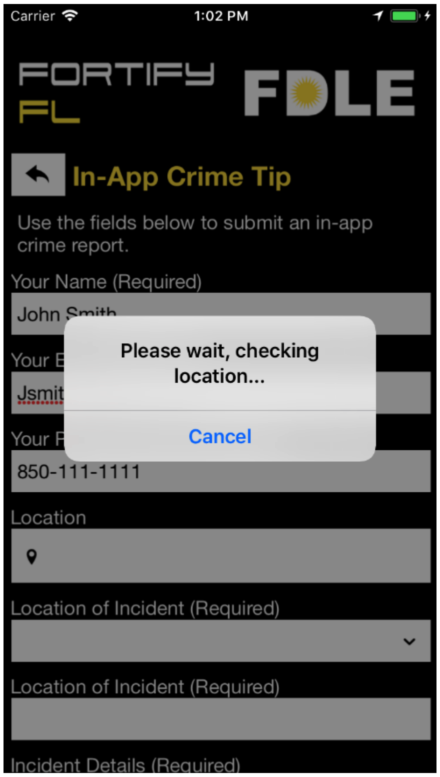
3.1 - A tip should require the user to select a school in Florida. This includes kindergarten through postsecondary, public and charter schools.

Any form fields can be made to be required in both the mobile app and website interface. In this context we would ensure that all schools in Florida are loaded into the system and that one must be selected in the event of a report. This sort of configuration can be made in real time via the content management system for the app and website. See concept images below.

3.2- School selection should be from a pick-list based on the geographic location of the user and minimizes the amount of searching required by the user.

AppArmor would achieve this for the State and FDLE via geofencing. On the AppArmor platform, the State and FDLE is able to create as many geo-fences as required to restrict or modify certain capabilities of the app based on the user's location. Geo-fences can also be applied at different layers of granularity, from the app in its entirety or down to a specific feature – such as reporting in this case. The platform in this context will reduce the number of options the user can submit a tip based on their current location. If they do not have location services enabled, then we will prompt the user to identify a certain geographical region of Florida and then reduce the available options based on their selection. The options will be sorted alphabetically.

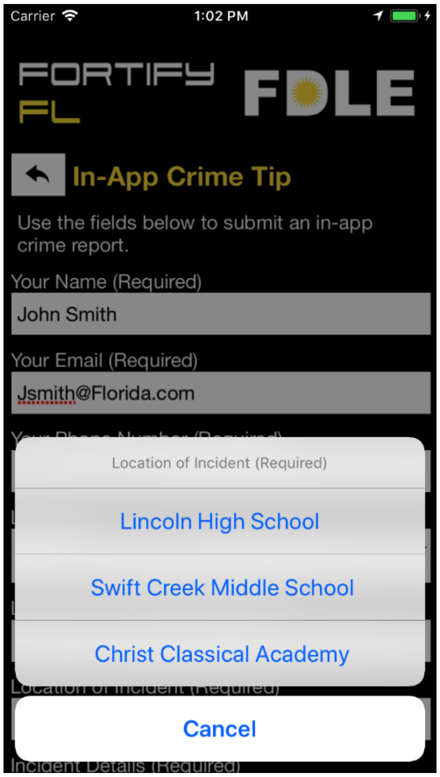
As an example (screenshots below), we created a geo-fence around the State for the Foritfy FL prototype app. We then simulated the user attempting to submit a report and the app determined the user's location and provided a more refined list of nearby schools. The user could then select from this list to submit their report.



Use the fields below to submit an in-app crime report.

Your Name (Required)
John Smith
Your E
Jsmit
Your P
850-111-1111
Location
Location of Incident (Required)
Location of Incident (Required)
Incident Details (Required)

Please wait, checking location...

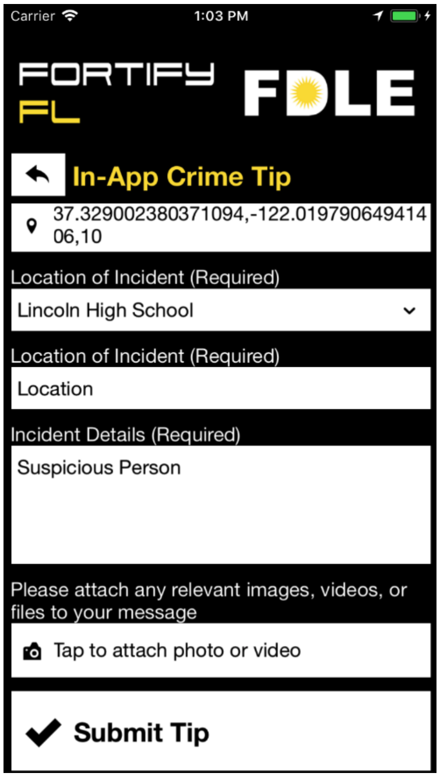


Use the fields below to submit an in-app crime report.

Your Name (Required)
John Smith
Your Email (Required)
Jsmith@Florida.com
Your Phone Number (Required)

Location of Incident (Required)

Location of Incident (Required)
Incident Details (Required)



37.329002380371094,-122.01979064941406,10
Location of Incident (Required)
Lincoln High School
Location of Incident (Required)
Location
Incident Details (Required)
Suspicious Person
Please attach any relevant images, videos, or files to your message

In the second scenario where the end user is not using location services, then the app prompts the end user to identify which geographic region of Florida they are currently in in order to narrow available reporting endpoints. After they choose their "region", options would be narrowed to the schools in the area.

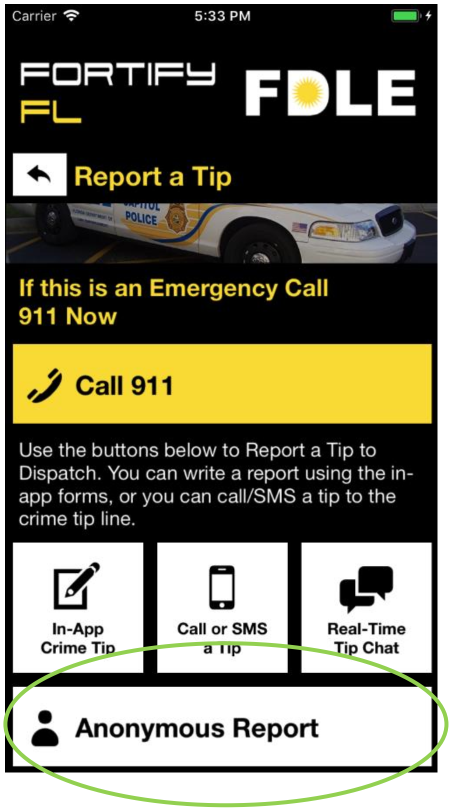
We'd encourage both options, as some users will refuse to use location services with the app.

3.3- Tips should include other relevant information such as type of tip, priority or alert level, and description of behavior or activity.

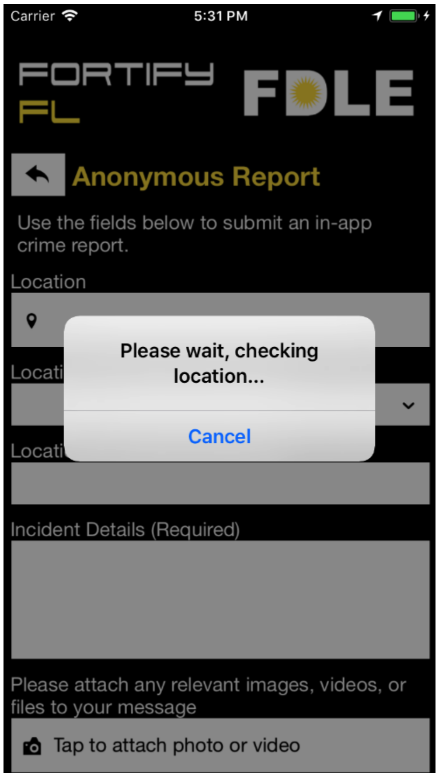
Any form fields can be made to be required in both the mobile app and website interface. In this context we would ensure that all the fields desired by the State are in place at the time of app launch. Note that these fields can be modified (made required or not, for example) or added and removed in real-time using the app and website content management system.

3.4- Users should have the option to submit tips anonymously or with identifying information.

Again, all fields can be made optional or required. For this request, we would simply make the “name” and all Personally Identifiable Information (PII) optional. Note that these fields can be modified (made required or not, for example) or added and removed in real-time using the app and website content management system. See image below of the menu with the fields removed:



Use the buttons below to Report a Tip to Dispatch. You can write a report using the in-app forms, or you can call/SMS a tip to the crime tip line.



Use the fields below to submit an in-app crime report.

Location

Locati

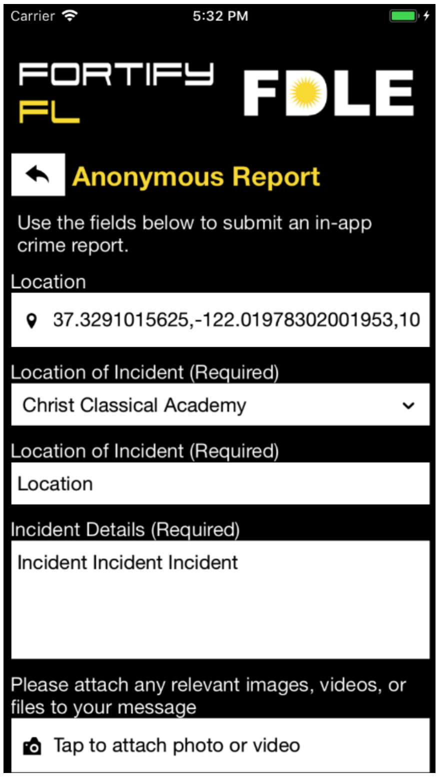
Locati

Incident Details (Required)

Please attach any relevant images, videos, or files to your message

Tap to attach photo or video

Please wait, checking location...



Use the fields below to submit an in-app crime report.

Location: 37.3291015625,-122.01978302001953,10

Location of Incident (Required): Christ Classical Academy

Location of Incident (Required): Location

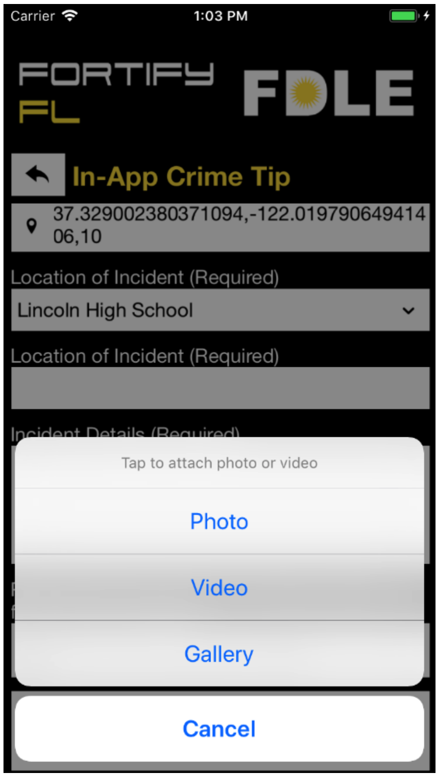
Incident Details (Required): Incident Incident Incident

Please attach any relevant images, videos, or files to your message

Tap to attach photo or video

3.5- Users should have the option to submit attachments with their tip, including images, video, audio, or document files.

Users are able to submit files from the device, such as previously recorded images in their gallery, videos, audio files, and documents on their device. We would want to ensure a file limit size for the convenience of the State (note that currently there is no restriction). End users can also “take” a photo or video or make a recording at the time of the report and then seamlessly attach it. See images below:



37.329002380371094,-122.01979064941406,10

Location of Incident (Required)
Lincoln High School

Location of Incident (Required)

Incident Details (Required)

Tap to attach photo or video

3.6- Contractor may propose other information to improve the functionality of the system.

The AppArmor Platform has over 50 powerful features, including advanced reporting capabilities. While these features are available to FDLE and the State, we have included them in Tab 6 as they are “optional” services in nature.

We are experts in mobile safety applications and would love to share our expertise with the State!

3.7- The system should send acknowledgement to the user that a tip has been received.

The user is provided an in-app message / confirmation message on the webpage after a tip has been successfully submitted and received by the authorities. We can supplement this ability if the end user has provided their contact information (either phone number or email address) in which we can send them any number of notification including:

- A confirmation SMS

- A confirmation email

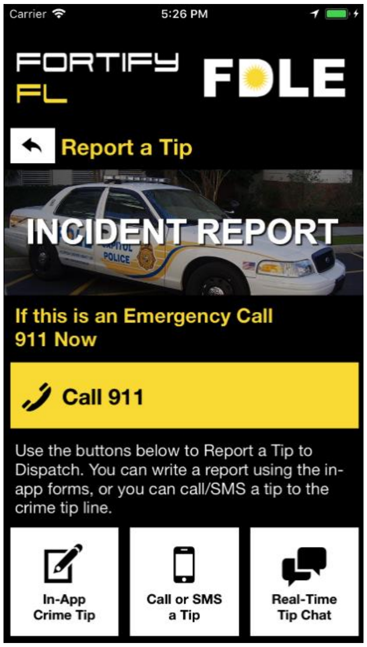
- A confirmation automated outbound call

These confirmation pages also include a unique confirmation number which can be used by the end user to view any previous reports. AppArmor is happy to investigate other options at the request of the State.

3.8- The system should prompt the user to call 9-1-1 if a tip involves an emergency or immediate threat.

Generally speaking, the way we've seen this deployed at hundreds of organizations is to provide a prompt prior to the end-user being able to fill in report form fields with a prompt of "If this is an emergency, call 911 immediately". We then provide that user a button which when tapped immediately calls 911.

At all times, we would ensure that the end user has the ability to quickly and effectively call 911 during a tip report.



If this is an Emergency Call 911 Now

Use the buttons below to Report a Tip to Dispatch. You can write a report using the in-app forms, or you can call/SMS a tip to the crime tip line.

3.9- The system should enable users to securely access tips they have submitted.

End users would be able to access their previously submitted tips via a confirmation number they received at the time of submitting their report to the State. They are then able to view all the details of their previous reports, add additional files or information, all of which are also sorted by date of submission.

AppArmor is happy to investigate other options at the request of the State should they have different preferred end user experience.

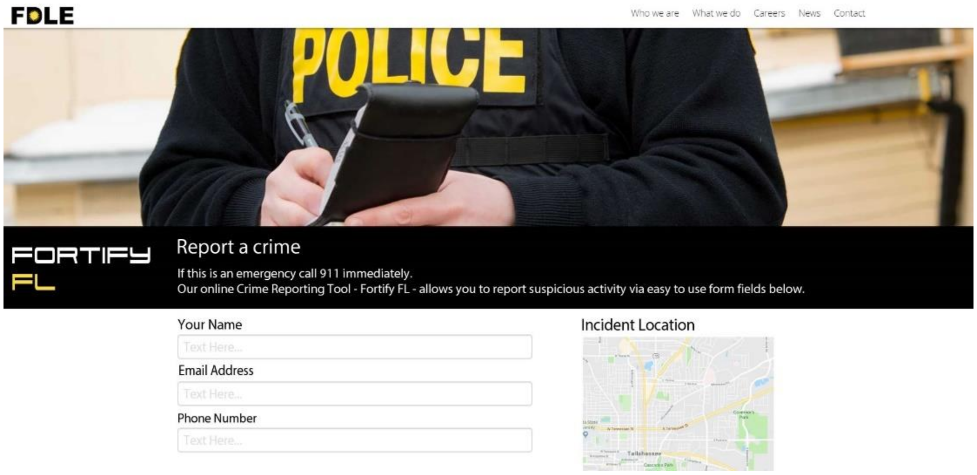
All reports are sent over SSL. Data is stored in an encrypted format at rest (TLS 1.2). Servers are on the Microsoft Azure geo-redundant platform with servers located in the United States. There is more on the security of the system in Tab 4 Part 2.

3.10- The system should allow users to add information or files to a tip after initial submission.

Consistent with the previous response, end users would be able to access their previously submitted tips via a confirmation number they received at the time of submitting their report to the State. They are then able to view all the details of their previous reports, add additional files or information, all of which are also sorted by date of submission.

3.11- The system should provide the ability for users that do not have a mobile device to submit a tip via a website.

The solution includes a custom branded reporting website with the same reporting options and fields as the mobile app. This webpage can be hosted by the State or AppArmor. Below is concept art of the page. Again, the reporting functionality will be in parity. In the administrative dashboard for the system, the origin of the



Report a crime

If this is an emergency call 911 immediately.
Our online Crime Reporting Tool - Fortify FL - allows you to report suspicious activity via easy to use form fields below.

Your Name
Text Here...

Email Address
Text Here...

Phone Number
Text Here...

Incident Location

4 – ROUTING TIPS

4.1 – The system should enable state and local administrators to specify the routing of tips.

In the administrative dashboard of the system all reports are identified in the "reports" page. In there, administrators responsible for their particular jurisdiction are able to send their reports to additional agencies or specific admin users as defined by the operation procedures of the State. This a configurable element of the dashboard which would be modified in collaboration with the State and FDLE. See section 4.3 for an image.

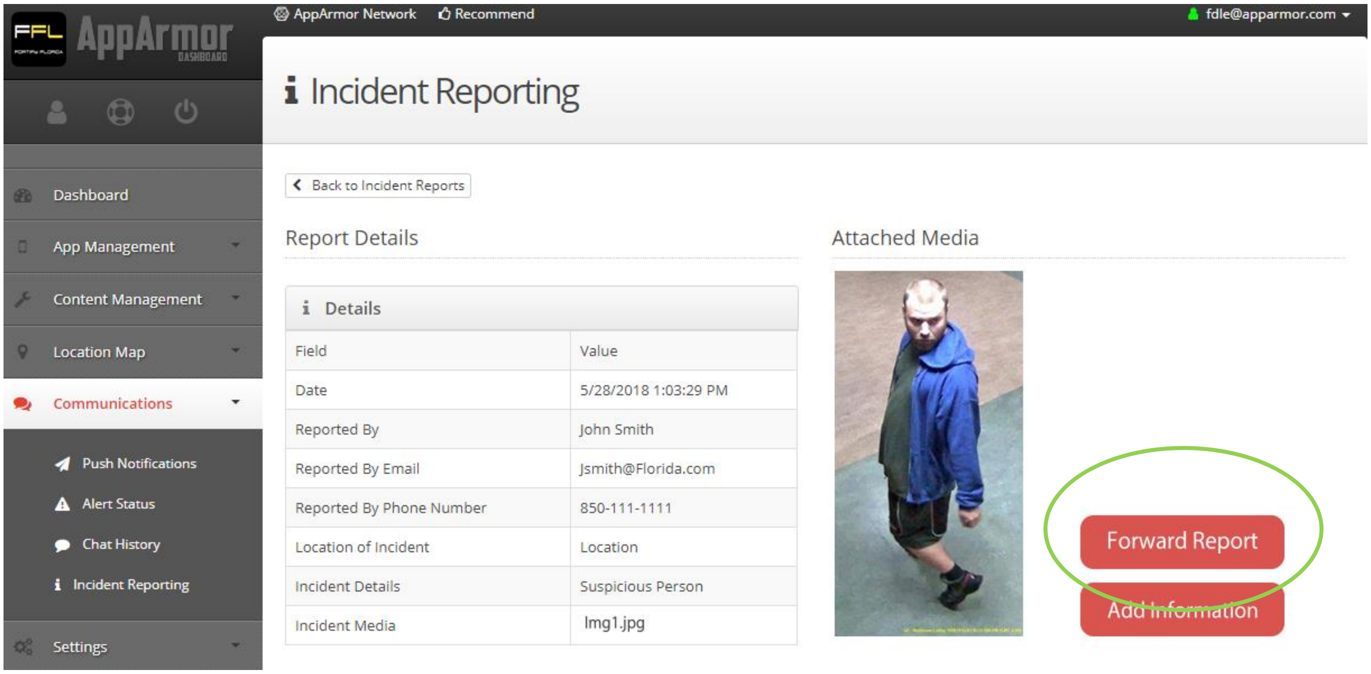
4.2 – The system should provide the ability for state and local administrators to enter contact information.

The administrative dashboard allows for any authorized administrative users to enter appropriate contact information on reports. Note that the reports will automatically be "stamped" with which administrator previously viewed it.

4.3 – The system should route tips to contacts specified by state and local administrators.

Tips received via the administrative dashboard can either be automatically routed or manually routed by appropriate staff as defined by their permissions in the online dashboard. For an automatic set up, this would be configured in advance and modifiable by certain super admin users of the dashboard. For manual routing, the individual receiving the report simply has to click the "forward report" button on the appropriate pages of the dashboard. See image below.

The system will then send a notification by email to the user receiving the report, notifying them of its arrival and displaying relevant content as well as notifying them in the administrative dashboard. Note that other alerting mechanisms, such as SMS notifications, push notifications, or others are also available.



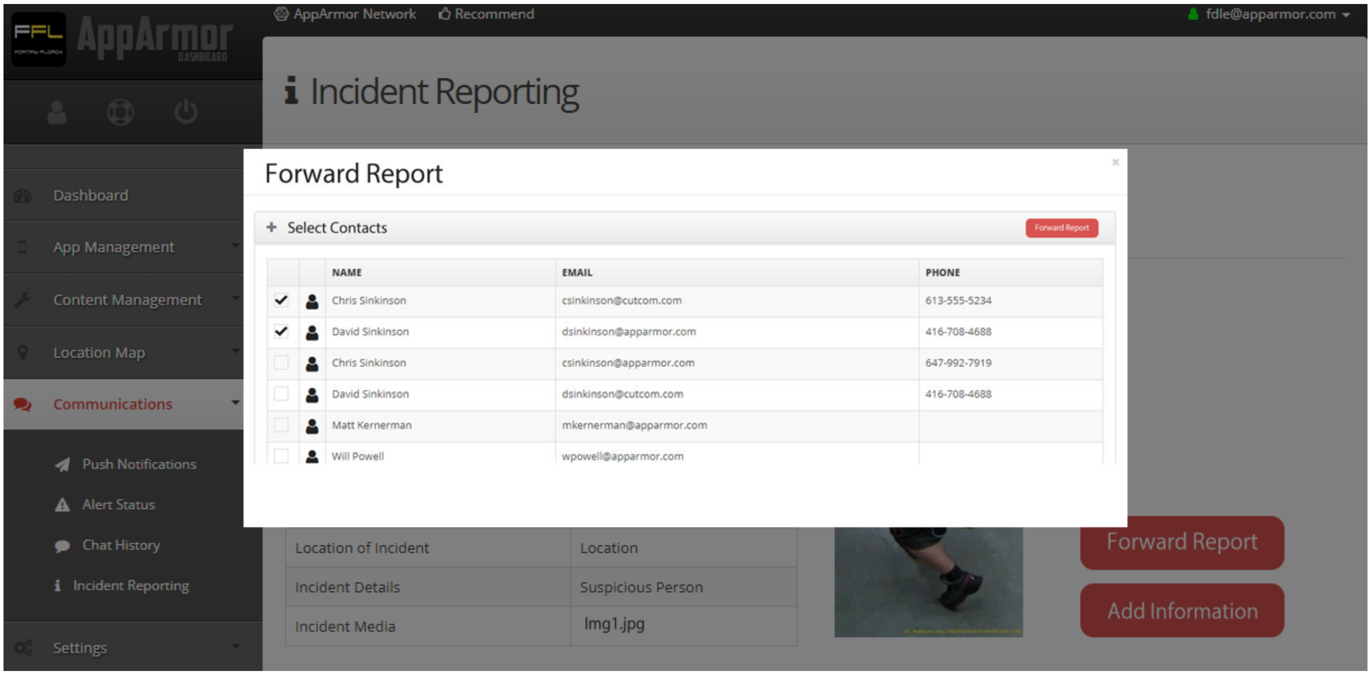
Incident Reporting

Report Details

Attached Media

Details

Field	Value
Date	5/28/2018 1:03:29 PM
Reported By	John Smith
Reported By Email	Jsmith@Florida.com
Reported By Phone Number	850-111-1111
Location of Incident	Location
Incident Details	Suspicious Person
Incident Media	Img1.jpg



Incident Reporting

Forward Report

+ Select Contacts

		NAME	EMAIL	PHONE
☑	👤	Chris Sinkinson	csinkinson@cutcom.com	613-555-5234
☑	👤	David Sinkinson	dsinkinson@apparmor.com	416-708-4688
□	👤	Chris Sinkinson	csinkinson@apparmor.com	647-992-7919
□	👤	David Sinkinson	dsinkinson@cutcom.com	416-708-4688
□	👤	Matt Kernerman	mkernerman@apparmor.com	
□	👤	Will Powell	wpowell@apparmor.com	

Location of Incident	Location
Incident Details	Suspicious Person
Incident Media	Img1.jpg

4.4 - All tips should be concurrently transmitted to FDLE's Office of Statewide Intelligence.

As noted in the previous response, reports can be automatically forwarded to any end point which the State and FDLE requires. This element would be configured in advance and modifiable by certain super admin users of the dashboard.

4.5 - The system should have the capability to transmit tips to state and local contacts by Email, FAX, message to the system management console, web service, or other similar means.

The following means are available to transmit tips to State and local contacts:

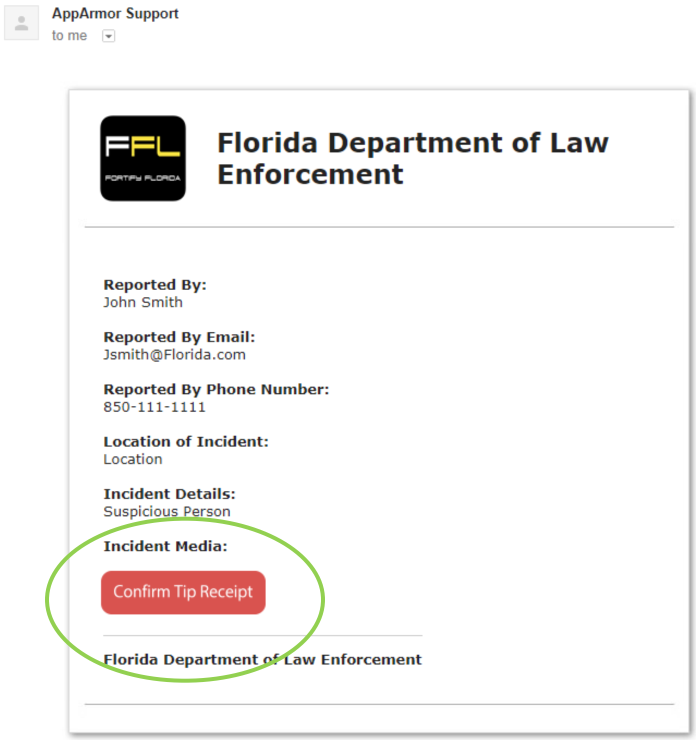
1. Email
2. Fax
3. SMS (Text)
4. Push Notification (via mobile app for FDLE users only and not the general public)
5. Message to system console (dashboard)
6. Automated outbound voice call
7. AppArmor Incident Reporting API (for third party systems)
8. RSS/ATOM feeds (for third party systems)

Should the State be interested in other options, AppArmor is willing to investigate and deploy them as necessary.

5 - CONFIRMATION OF RECEIPT

5.1 - The system should enable specified local agency contacts to confirm receipt of a tip.

The AppArmor Dashboard will maintain the list of both education institutions and their appropriate contacts as well as related local agency contacts, and the contact information of larger state-wide agency personnel. These personnel then confirm receipt in one of many forms – either via the administrative dashboard prompt, or in the specific alerting mechanisms through which they received the report. For instance, in the example below, the user received the tip report via email and could indicate in that email that they confirmed receipt:



AppArmor Support
to me

Florida Department of Law Enforcement

Reported By:
John Smith

Reported By Email:
Jsmith@Florida.com

Reported By Phone Number:
850-111-1111

Location of Incident:
Location

Incident Details:
Suspicious Person

Incident Media:

Florida Department of Law Enforcement

This then identifies in the administrative dashboard to all related parties that the report has been acknowledged.

5.2 - Should receipt of a tip not be confirmed within TBD minutes, the system should transmit a second notice to contacts specified by local agency administrators.

Automated protocols for confirmation escalation can be easily configured in the system. Certain logical rules, such as “Send email if a tip has not been confirmed in 5 minutes” can be added at the time of onboarding and changed after-the-fact to meet operational objectives. Thus, this can easily be accomplished on the platform.

5.3 - Should receipt of second notice not be confirmed within TBD minutes, the Contractor should confirm receipt by initiating a telephone call the specified local agency contact(s).

As was noted in the previous question and in question 4.5, logical rules can be added to ensure confirmation of a report. Then the available mechanisms, such as in this case outbound calling, can be utilized to repeatedly notify appropriate administrative users to confirm receipt of the report.

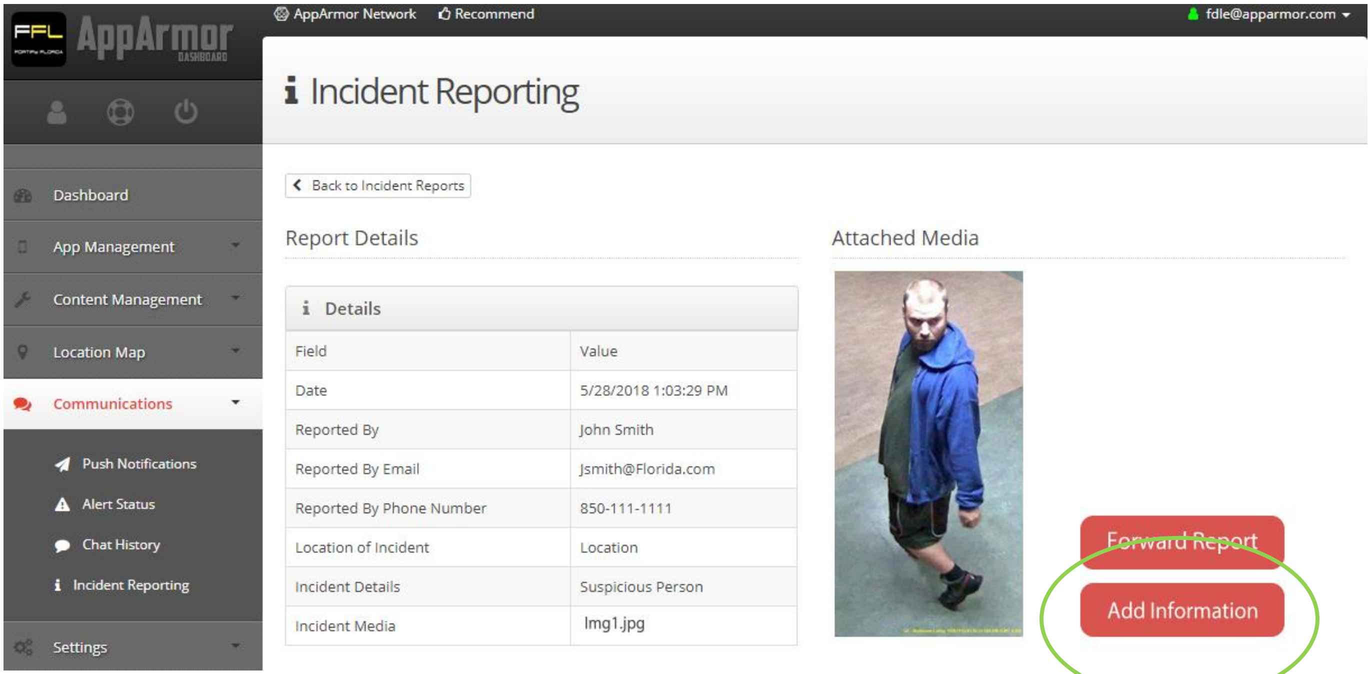
Further, multiple mechanisms can also be utilized to notify particular administrative users during an escalation. As an example, an administrative user can be sent both a text message and an outbound call simultaneously, if that's something which the state is interested in.

This is a common request of our alerting software, which is a related product line to the AppArmor Safety reporting software. Frequently we'll use outbound calling to "hunt" for the appropriate individual at an organization during an emergency.

6 - UPDATE STATUS

6.1 - The system should provide agencies with the ability update status of a tip.

The online dashboard allows for administrative users with appropriate levels of access to provide updates and "notes" to existing reports. Viewing restrictions on these notes can also be applied so that only appropriate staff can view the information added by particular agencies. Below is a screenshot of the button to add a note:



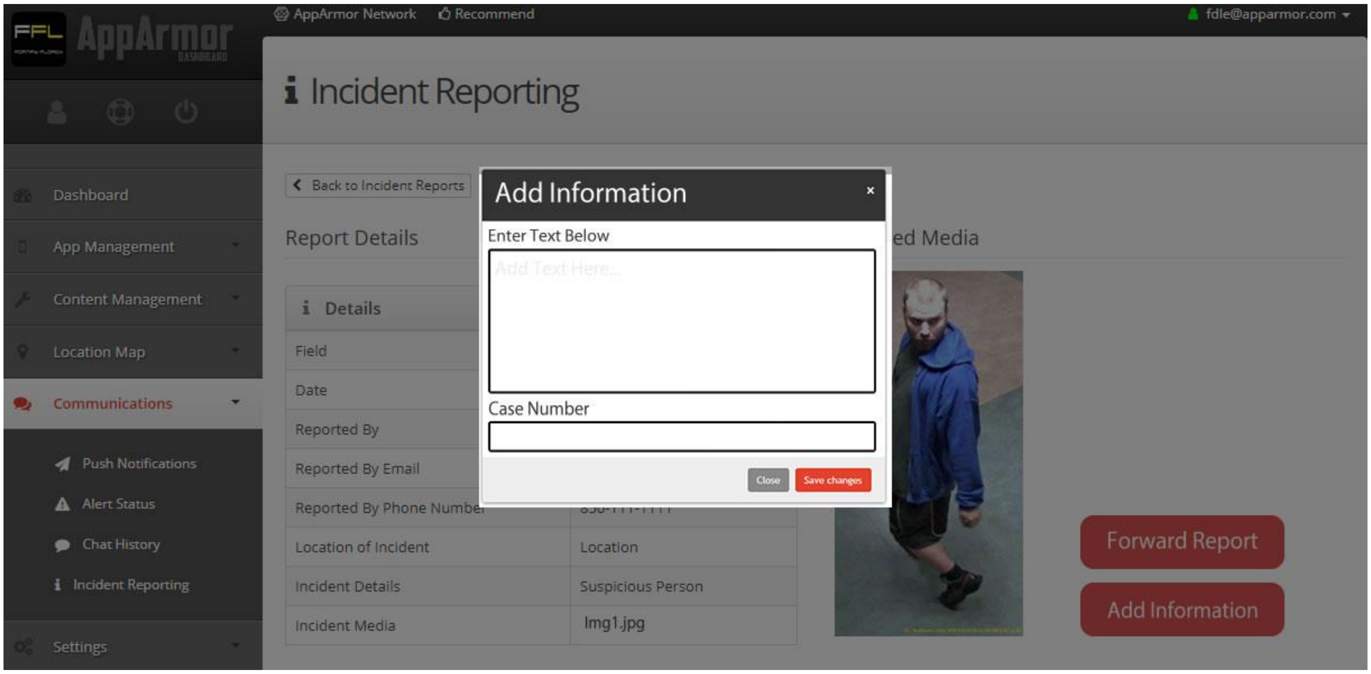
Incident Reporting

Report Details

Details

Field	Value
Date	5/28/2018 1:03:29 PM
Reported By	John Smith
Reported By Email	Jsmith@Florida.com
Reported By Phone Number	850-111-1111
Location of Incident	Location
Incident Details	Suspicious Person
Incident Media	Img1.jpg

Updates can also be made to the status of tips. Currently tips have three statuses "Open, Under Review, and Closed"; these statuses can be modified by admin users. Lastly, while those three status are the only current options, additional statuses can be added at the request of the State.



Incident Reporting

Report Details

Add Information

Enter Text Below

Add Text Here...

Case Number

ed Media

Details	
Field	
Date	
Reported By	
Reported By Email	
Reported By Phone Number	850-111-1111
Location of Incident	Location
Incident Details	Suspicious Person
Incident Media	Img1.jpg

6.2 - The system should provide agencies with the ability to enter case numbers.

Additional fields from an administrative perspective for reports can be configured by appropriate staff of the State and FDLE. As a result, adding a "case number" field is very much available for the State. An image of such a configuration was included in the previous answer.

7 - RECORD MAINTENANCE

7.1 - The system should maintain audit logs of events associated with tips, including receipt, routing, confirmation, and status update.

As AppArmor is currently active in numerous municipal, state and federal jurisdictions, the need to provide a flexible reporting audit history (logs) is something that is at the core of our business. As a result, the system logs all information regarding a report – receipt, routing/actions, confirmation, statuses, and content (including media) – at the length legally required in the jurisdiction.

7.2 - Ownership of tips and associated files should reside with the State of Florida.

Agreed. The State is the owner of all tips and associated files. AppArmor owns all software developed and licenses it to the State and FDLE as required.

7.3 - Tips and associated files should be maintained in the system per the Florida Public records requirements.

All tips and reports will be maintained per the Florida Public records requirements and subject to regular review by the State to ensure exact compliance. AppArmor is extremely interested in ensuring that it following, with extreme accuracy, the exact laws as required in the State for tips and reporting information.

With that stated, AppArmor does already work with numerous agencies in the State who regularly have tip reports flowing through the AppArmor system. As a result, we're confident that we currently meet the guidelines of the State.

7.4 - Upon termination of the contract, the Contractor should deliver to FDLE an electronic copy of all tips and associated files in a manner specified by FDLE.

AppArmor will, upon termination of the contract, deliver to FDLE an electronic copy of all tips and associated files specified by FDLE.

7.5 - Following FDLE's confirmation of receipt of the electronic copy, the Contractor should destroy all records of tips and associated files. Following destruction of these records, the Contractor should deliver written certification to FDLE that all records have been destroyed.

AppArmor will, after confirming that files have been successfully transferred to FDLE and the State, destroy all records of tips and associated files on AppArmor systems. AppArmor will then provide a destruction certification to FDLE to confirm that all records have been destroyed and optionally offer FDLE staff the opportunity to confirm that all files were deleted by giving appropriate access to AppArmor systems.

8 - MANAGEMENT CONSOLE / DASHBOARD

8.1 - The system should provide a management console / dashboard for use by state and local agency administrators.

The State, FDLE, and all applicable administrators will have access to the online dashboard in order to view the reports specific to their jurisdiction. The console is a cloud-based system available 24/7/365 and housed on the Microsoft Azure Geo-Redundant platform with servers located in the United States.

Azure has more certifications than any other cloud provider and leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, such as Criminal Justice Information Services (CJIS) and more.

Rigorous third-party audits, verify Azure's adherence to the strict security controls these standards mandate. AppArmor benefits from the powerful security measures enacted by the Azure platform.

8.2 - The management console / dashboard must provide functions described below:

8.2.1 - Create, update, and delete contact information.

The dashboard makes it possible for administrative users to modify their contact information via their profile. Users can create, update, and delete contact information as required.

8.2.2 - Specify routing of tips within a county and agency.

As was demonstrated in question 4.3, administrative users would be able to specify the routing of tips manually to certain end users at available agencies in a searchable list of contacts. However, automated routing can also be configured as required.

8.2.3 - Export individual tips and attached files.

All tips, or individual tips can be both viewed or exported from the dashboard including their attached media (audio, picture or video files). The available formats for the reports is .csv and .xlsx although other mechanisms are available and may be required given the size of the report in question (due to increasingly large video sizes).

8.2.4 - Perform basic searches.

Basic searching of tips, based on keywords such as reported details (name, email address, phone number) or incident details, or case number. Generally speaking, any reported information can be searched via the searching tool in the interface.

8.2.5 - Perform complex searches (such as Boolean and fuzzy string searching).

Fuzzy searches and "advanced" search options are also available. These are usually configured to the specific needs of the partner organization, and thus can vary by organization. Similar examples however would be partially complete phone numbers or names, or using multiple search parameters, such as narrowing the search to a specific set of dates and then also searching by phone number as an example.

8.2.6 - Run reports.

Exhaustive reporting is also available via the system. This includes viewing all active reports, time open, average time till completion and more. Additional reporting functionality can be added for the State as required in order to meet operational response time objectives.

8.2.7 - Extract files.

Similar to the answer in 8.2.3, all tips or files can be exported from the system. Additional details around file extraction would be required in order to implement additional options for the State and FDLE.

TAB 4 – TECHNICAL (NON-FUNCTIONAL)

Below we've responded to the appropriate Functional Requirements per the ITN, Attachment F Section II, part C3.

1 - PROJECT MANAGEMENT

1.1 - While FDLE assumes primary responsibility for preparing project management documentation, the Contractor should work with FDLE to produce and maintain project management documentation in accordance with FDLE's IT Project Management Standards.

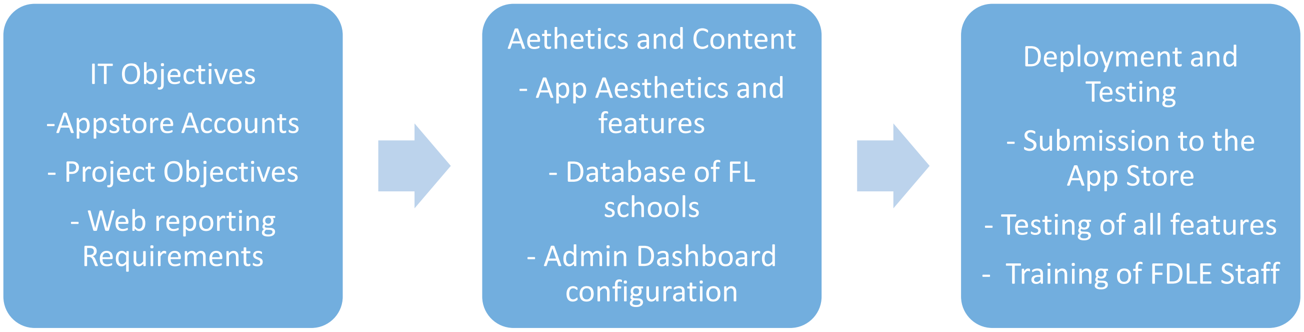
Absolutely. For all AppArmor deployments, a collaborative project plan with actionable timelines and meaningful deadlines is executed. Below we've outlined our proven process which has been successful at over 170 organizations across the globe.

1.1.1 - Project Plan Details

AppArmor has had great success implementing fully customized apps with advanced reporting options for over 170 organizations across the globe. Among the most important stages is the establishment of the project plan and timelines. This is when we establish the roadmap and important objectives which have to be achieved by AppArmor or The State and FDLE.

Will Powell, Sr. Manager of Operations at AppArmor and our most senior project manager will have direct oversight of this project and will act as they key contact to manage technical and operational elements of the implementation. Will has successfully deployed numerous apps and mass notification projects for AppArmor at institutions across the globe, including those of similar scope to The State and FDLE (i.e. Kansas Safe Schools, New York University, the Colorado Community College System, and more), in which he managed technical and operational elements to coordinate institutional specific resources and content to increase functionality and ease of use for end-users.

In coordination with the FDLE implementation team and other key stakeholders, Will Powell will both break down the project into more digestible sub projects and establish key timelines based on the needs and priorities of The State and FDLE. There are three distinct phases to any reporting app deployment. They are:



IT Objectives

-Appstore Accounts

- Project Objectives

- Web reporting Requirements

Aethetics and Content

- App Aesthetics and features

- Database of FL schools

- Admin Dashboard configuration

Deployment and Testing

- Submission to the App Store

- Testing of all features

- Training of FDLE Staff

a. IT Objectives: This involves getting access to the The State/FDLE's appstore accounts so that AppArmor may submit the app under the The State and FDLE account. This stage, while seemingly trivial, is essential as having the app in the State's appstore accounts will ensure both higher downloads and that the state wholly owns all end-user data. We are happy to further comment on this important point at in discussions with the State.

It is worth noting that this a unique benefit of our platform. It is highly unlikely any other organization would be willing to submit the app under the appstore accounts of the State. Aside from the benefits as outlined above, it also gives the State greater flexibility down the road should it wish to switch vendors.

As this project will also require the deployment of a webpage for incident reporting (which can be executed concurrently to getting access to appstore accounts and will likely be mostly executed by AppArmor) we would begin the early stage of identifying where the page is located and what resourcing needs are required from the State and FDLE.

b. Aesthetic and Content Objectives: This phase requires the The State and FDLE's marketing department to confirm app Aesthetics with the AppArmor design team (generally this is a very quick task). Secondly, this phase also incorporates determining the layout of the app as it pertains to content and features. This is a very exciting phase where your reporting app solution comes together and ensures a smooth end-user experience.

Further, it is at this stage where the database of Florida Institutions is added to the platform for the purposes of easing end user tip routing via geofencing. That is, this stage will include the configuration of the capability for the app to decide which agency should receive tip reports based on the end-user's location.

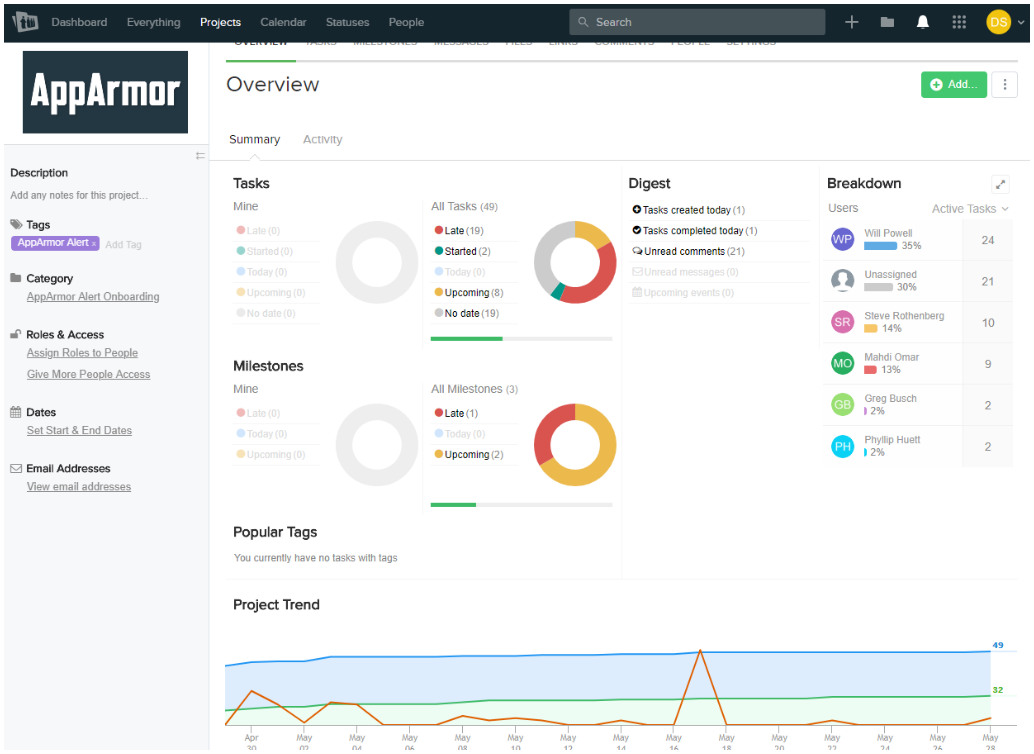
c. Deployment and Testing: Once phases A and B have been completed AppArmor will submit the app to the appropriate appstores. The app will be under review with Apple for 1-5 business days and live within 4 hours for Google. After the apps are live, we will move quickly to test the push notification capabilities to ensure the launch was successful.

1.2 - Requirements Validation Document Template

AppArmor would coordinate closely with the state in ensuring that the requirements of the product are added to our project management software, Teamwork. Project managers at FDLE would have access to the system at any time and be able to view and manage the required tasks for themselves, their colleagues and AppArmor. This is a fantastic platform for creating accountability and visibility on to the current status of a project. More information is provided in the next answer.

1.3 - The Contractor should assist FDLE in producing and maintaining a Requirements Traceability Matrix.

FDLE staff would be invited to the Teamwork project and able to track the current status of any element of the project. These objectives would be established based on AppArmor's best practices with other app deployments as well as input from the FDLE. A "Kickoff Call" would establish a high level project overview where requirements are established, along with essential tasks. Then, deadlines and key personnel would be assigned to these tasks. An overview would be visible at any time via the Teamwork platform:



Overview

Description
Add any notes for this project...

Tags
AppArmor Alert × Add Tag

Category
AppArmor Alert Onboarding

Roles & Access
Assign Roles to People
Give More People Access

Dates
Set Start & End Dates

Email Addresses
View email addresses

Tasks

Mine	All Tasks (49)
Late (0)	Late (19)
Started (0)	Started (2)
Today (0)	Today (0)
Upcoming (0)	Upcoming (8)
No date (0)	No date (19)

Milestones

Mine	All Milestones (3)
Late (0)	Late (1)
Today (0)	Today (0)
Upcoming (0)	Upcoming (2)

Digest
- Tasks created today (1)
- Tasks completed today (1)
- Unread comments (21)
- Unread messages (0)
- Upcoming events (0)

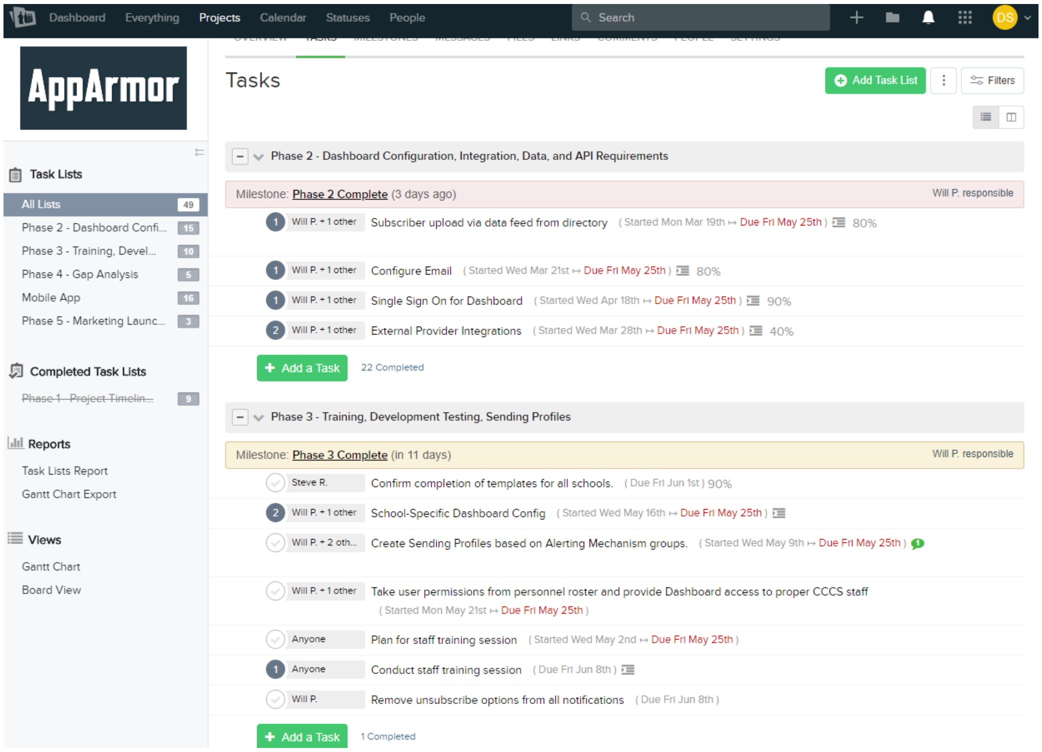
Breakdown

Users	Active Tasks
WP Will Powell 35%	24
Unassigned 30%	21
SR Steve Rothenberg 14%	10
MO Mahdi Omar 13%	9
GB Greg Busch 2%	2
PH Phyllip Huett 2%	2

Popular Tags
You currently have no tasks with tags

Project Trend

Above is an example of dashboard for a mobile app project.



Tasks

Phase 2 - Dashboard Configuration, Integration, Data, and API Requirements

Milestone: Phase 2 Complete (3 days ago) — Will P. responsible

- 1 | Will P. + 1 other | Subscriber upload via data feed from directory (Started Mon Mar 19th ↦ Due Fri May 25th) 80%
- 1 | Will P. + 1 other | Configure Email (Started Wed Mar 21st ↦ Due Fri May 25th) 80%
- 1 | Will P. + 1 other | Single Sign On for Dashboard (Started Wed Apr 18th ↦ Due Fri May 25th) 90%
- 2 | Will P. + 1 other | External Provider Integrations (Started Wed Mar 28th ↦ Due Fri May 25th) 40%

+ Add a Task — 22 Completed

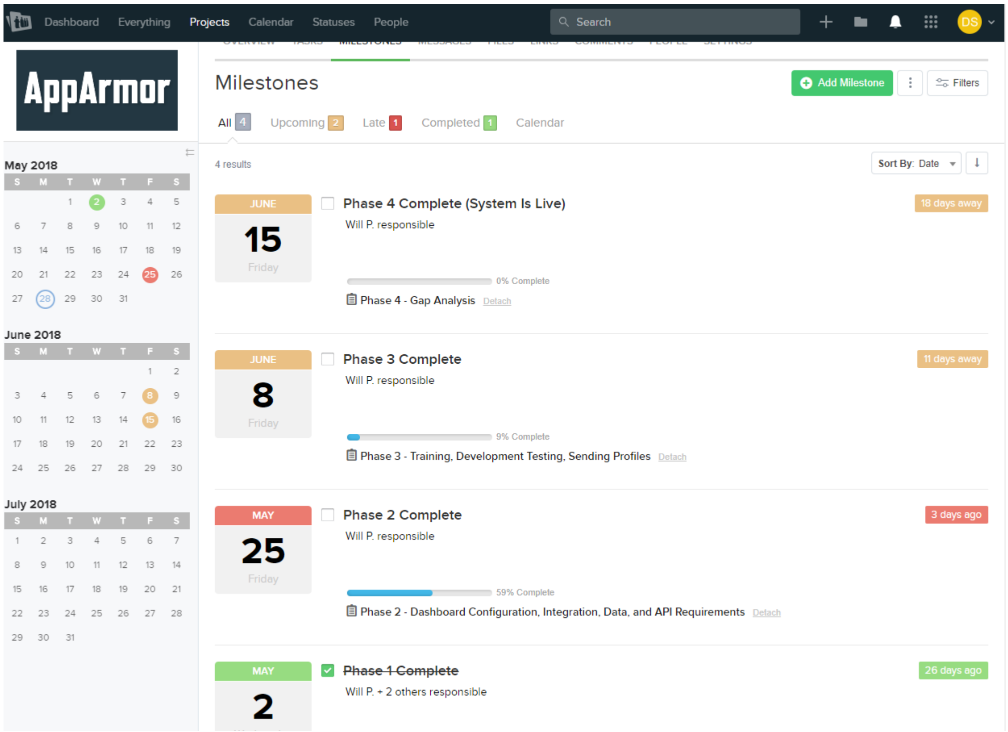
Phase 3 - Training, Development Testing, Sending Profiles

Milestone: Phase 3 Complete (in 11 days) — Will P. responsible

- Steve R. | Confirm completion of templates for all schools. (Due Fri Jun 1st) 90%
- 2 | Will P. + 1 other | School-Specific Dashboard Config (Started Wed May 16th ↦ Due Fri May 25th)
- Will P. + 2 oth... | Create Sending Profiles based on Alerting Mechanism groups. (Started Wed May 9th ↦ Due Fri May 25th) 1
- Will P. + 1 other | Take user permissions from personnel roster and provide Dashboard access to proper CCCS staff (Started Mon May 21st ↦ Due Fri May 25th)
- Anyone | Plan for staff training session (Started Wed May 2nd ↦ Due Fri May 25th)
- 1 | Anyone | Conduct staff training session (Due Fri Jun 8th)
- Will P. | Remove unsubscribe options from all notifications (Due Fri Jun 8th)

+ Add a Task — 1 Completed

Above is an example of deadlines in particular phases of a mass notification project.



May 2018

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

June 2018

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

July 2018

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Milestones

4 results

JUNE 15 Friday — □ **Phase 4 Complete (System Is Live)** — 18 days away
Will P. responsible
0% Complete
Phase 4 - Gap Analysis Detach

JUNE 8 Friday — □ **Phase 3 Complete** — 11 days away
Will P. responsible
9% Complete
Phase 3 - Training, Development Testing, Sending Profiles Detach

MAY 25 Friday — □ **Phase 2 Complete** — 3 days ago
Will P. responsible
59% Complete
Phase 2 - Dashboard Configuration, Integration, Data, and API Requirements Detach

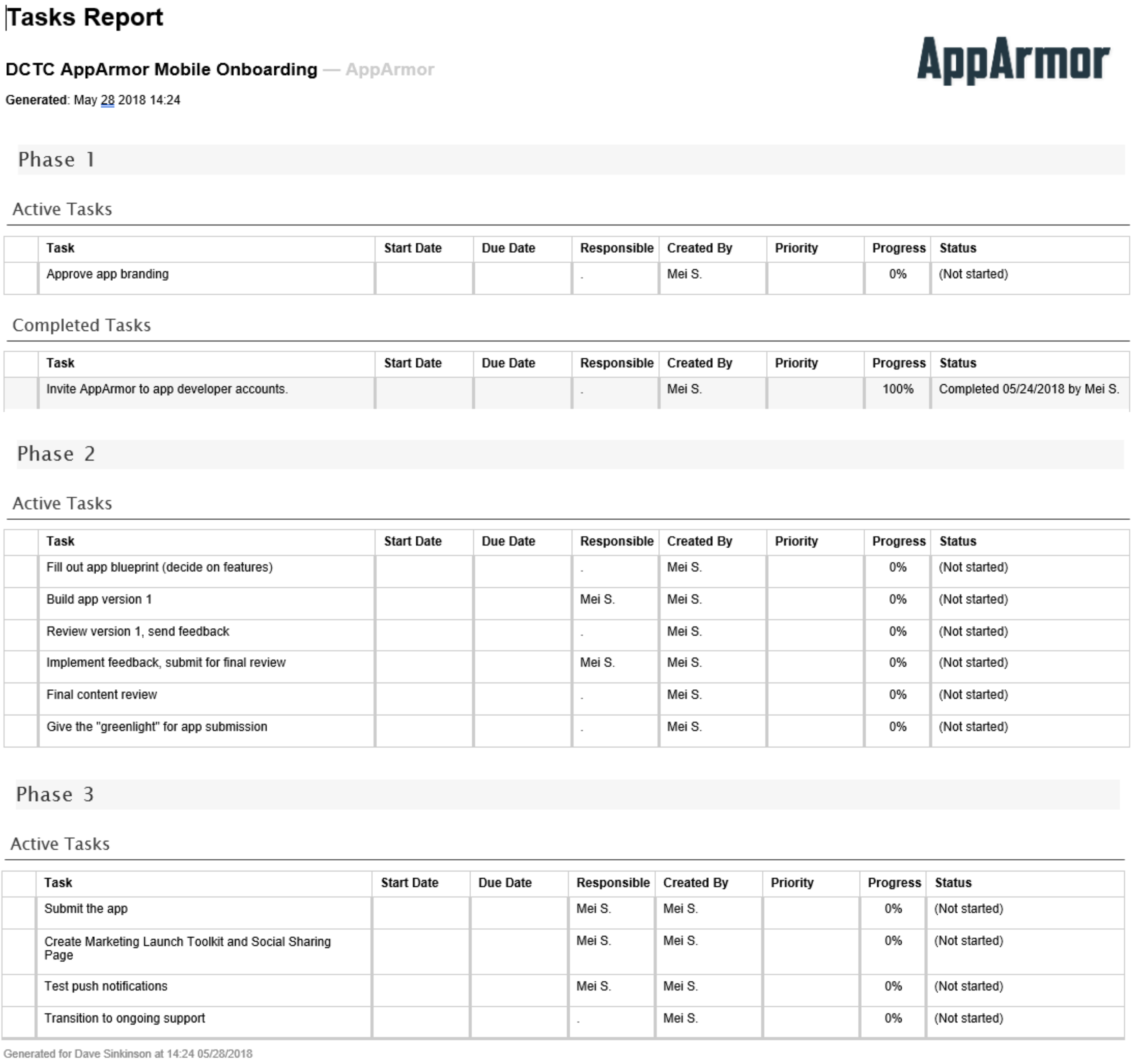
MAY 2 — ☑ ~~**Phase 1 Complete**~~ — 26 days ago
Will P. + 2 others responsible

Above is an example of major milestones in particular phases of a mass notification project.

1.4 - The Contractor should prepare an Implementation Plan.

The “high level” of the implementation plan was listed in answer 1.1 of this Tab. We would be happy to additionally coordinate with staff at FDLE to coordinate the details of and execute the implementation plan. Generally speaking, previous plans have been based on our hundreds of successful deployments across the globe.

Below is an example of the common tasks for a mobile app with advanced reporting implementation plan:



Tasks Report

DCTC AppArmor Mobile Onboarding — AppArmor

AppArmor

Generated: May 28 2018 14:24

Phase 1

Active Tasks

	Task	Start Date	Due Date	Responsible	Created By	Priority	Progress	Status
	Approve app branding			.	Mei S.		0%	(Not started)

Completed Tasks

	Task	Start Date	Due Date	Responsible	Created By	Priority	Progress	Status
	Invite AppArmor to app developer accounts.			.	Mei S.		100%	Completed 05/24/2018 by Mei S.

Phase 2

Active Tasks

	Task	Start Date	Due Date	Responsible	Created By	Priority	Progress	Status
	Fill out app blueprint (decide on features)			.	Mei S.		0%	(Not started)
	Build app version 1			Mei S.	Mei S.		0%	(Not started)
	Review version 1, send feedback			.	Mei S.		0%	(Not started)
	Implement feedback, submit for final review			Mei S.	Mei S.		0%	(Not started)
	Final content review			.	Mei S.		0%	(Not started)
	Give the "greenlight" for app submission			.	Mei S.		0%	(Not started)

Phase 3

Active Tasks

	Task	Start Date	Due Date	Responsible	Created By	Priority	Progress	Status
	Submit the app			Mei S.	Mei S.		0%	(Not started)
	Create Marketing Launch Toolkit and Social Sharing Page			Mei S.	Mei S.		0%	(Not started)
	Test push notifications			Mei S.	Mei S.		0%	(Not started)
	Transition to ongoing support			.	Mei S.		0%	(Not started)

Generated for Dave Sinkinson at 14:24 05/28/2018

1.5 - The Contractor should take part in weekly status meetings during implementation of the system.

AppArmor would be happy to participate in weekly status meeting during the implementation of the system. In fact, we'd insist on this level of accountability in order to ensure that all needs of the State and FDLE are met.

2 - SECURITY

2.1 - Contractor will conform to Rule 74-2, Florida Administrative Code (Florida Cybersecurity Standards)

Upon review of Rule 74-2 of the Florida Administrative Code (Florida Cybersecurity Standards) which establish minimum standards to be used by state agencies to secure IT resources across five high-level functions: Identify, Protect, Detect, Respond, and Recover, we can confirm that AppArmor currently conforms with the rule. That said, AppArmor would be happy to execute a security review of our systems to ensure that we continue to be in compliance and identify areas of possible improvement. Security is paramount and we take it exceptionally seriously.

2.2 - Contractor should ensure that policies and procedures for securing Florida information and system resources are in place and understood by all affected parties

From a file/data security profile, AppArmor is extremely robust. All communications to and from the reporting system to the dashboard or mobile app are over SSL. At rest, data is stored in an encrypted format (TLS 1.2). Data is located in US Data Centers at various locations across the US. The console is a cloud-based system available 24/7/365 and housed on the Microsoft Azure Geo-Redundant platform. Azure also provides continuous upstream attack pattern protection, meaning that on top of our infrastructure is additional security from our hosting provider.

Azure has more certifications than any other cloud provider and leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, such as Criminal Justice Information Services (CJIS) and more.

Our systems are also monitored in real-time monitoring by AppArmor support staff. In all, numerous steps are taken to protect the data of our partners.

2.3 - Contractor should ensure that security controls are in place to minimize risks to the confidentiality, integrity, and availability of the system and data.

From the perspective of access security, AppArmor closely follows industry best practices. Access to information in the system based on user roles and associated access rights. Access to data is assigned on the principle of "Least Privilege" and managed according to AppArmor documented procedures. Employees are required to sign NDAs at time of hiring and all information is owned by the partner organization. Data is not shared with third parties, unless at the request of the partner organization. Data is wholly owned by the State.

In terms of availability of the system, our uptime SLAs is 99.95%.

2.4 - The system must be compliant with HIPAA and FERPA.

The system is fully compliant with HIPAA and FERPA.

2.5 - All data should be encrypted in transit using TLS 1.2 or higher, with minimum cypher strength of 128 bits (AES 256 preferred).

All communications to and from the reporting system to the dashboard or mobile app are over SSL. At rest, data is stored in an encrypted format (TLS 1.2). AES 256 is also available and will be implemented for this solution.

2.6 - Access to information in the system should be based on user roles and associated access rights. Access should be assigned on the principle of "Least Privilege" and managed according to documented procedures.

The AppArmor dashboard, of which the State would have unlimited accounts is restricted based on certain user roles and permissions. The permissions can be granular – access restricted to certain reports in the dashboard – or global, with entire options simply not being available. By default, administrative users start with only limited access to content relevant to their reporting jurisdiction. Below is an image of the user permissions page.

Furthermore, AppArmor staff members assigned to the project are the only individuals permitted to access the relevant files and documentation as required for the deployment of the software. This access is also governed by internal documentation at AppArmor which can be provided upon request.

2.7 - System resources should be protected by physical controls. Contractor should maintain procedures to manage physical access to information technology facilities housing Florida information.

All physical access to the systems is managed by Microsoft. Indeed, to ensure security, even AppArmor staff do not have access to the datacenter. On the Azure Trust Center website, Microsoft identifies the following physical access security measures taken:

> *"The first layer of physical security starts with requesting access prior to arriving at the datacenter. You must provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. This is to help keep the number of individuals needed to complete a task in our datacenters to the bare minimum. Once permissions are granted, an individual only has access to the discrete area of the datacenter based on the approved business justification. Permissions are limited to a certain period of time and expire after the allowed time period.*
>
> *The next layer of security is the building's perimeter. At a datacenter, you must go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team monitoring their videos 24/7 and 365 days of the year.*
>
> *Once you gain access to the datacenter's perimeter, you must pass additional security measures to enter the datacenter. The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter while they also monitor the videos of cameras inside the datacenter 24/7 and 365 days a year. After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter the portion of the datacenter that you have approved access to and can stay there only for the duration of the time approved.*
>
> *Once you arrive at the entrance to the requested part of the datacenter floor, you must pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every virtual machine rack. Everything that you will do with your virtual machine will be tracked—the first time a hard disk goes into a virtual machine until it is cleaned and erased. Full body metal detection screening is*

> *repeated when you exit the datacenter floor. To leave the datacenter, you have to pass through an additional security scan."*[1]

In collaboration with Microsoft, AppArmor is able to offer world class physical security protocols which would protect the State's data.

2.8 - Contractor should implement procedures to protect Florida information from loss, destruction, and unauthorized or improper disclosure or modification.

AppArmor performs daily backups of all data which is kept off-site. We also mirror all data to secondary datacenters. Data can be restored when needed by our staff. Our data management policy also mandates that we "flag as deleted" rather than fully delete in most instances. This means that we can often un-delete any data fairly quickly.

2.9 - Logical controls should be in place to segregate and protect Florida's information.

All of Florida's data is kept in isolation and can be exported or destroyed as necessary.

2.10 - Contractor should notify FDLE of any suspected cybersecurity incident or breach of Florida information within 24 hours of discovery.

AppArmor will notify FDLE of any breach of suspected incident or breach within 2 hours of discovery, as that is our standard policy. At that time, AppArmor will approach the State with a report on the incident, consequents, and a proposed action plan. The State will be notified by email and phone call, with the intention to schedule a contact point within the 2-hour timeframe.

2.11 - Data Confidentiality and Exemptions based on Florida State Law and Constitution.

AppArmor will conform with all data confidential and exemptions based on Florida State Law and the Constitution of the State. AppArmor would look to the State to confirm that the firm is in compliance.

[1] https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/

3 – SYSTEM SUPPORT

3.1 - The system will be designed and developed to support a 24/7 production environment and reporting system.

The console is a cloud-based system available 24/7/365 and housed on the Microsoft Azure Geo-Redundant platform. The mobile app as well is a 24/7/365 system with no downtime. In terms of availability of the system, our uptime SLAs is 99.95%.

3.2 - Contractor should ensure that software products used in the system (e.g., operating systems, web server platforms, database management, development frameworks) are upgraded or replaced prior to reaching end-of-life or unsupported status.

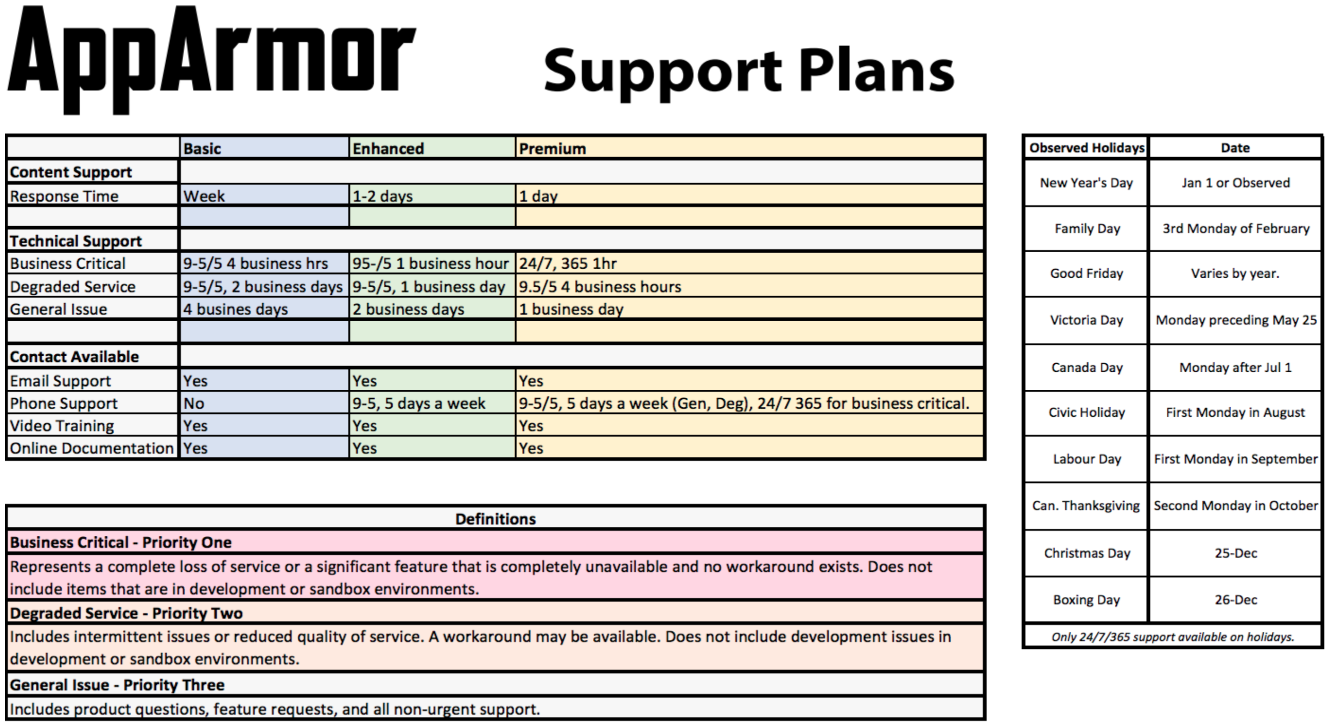
Our systems are automatically upgraded by Microsoft Azure as necessary. We do not operate any software reaching an end-of-life or unsupported status.

3.3 - The Contractor will provide a Help Desk that is available during FDLE business hours (Monday - Friday, 8:00 a.m. - 6:00 p.m. Eastern Time) to assist with usability questions, problem analysis and for reports of technical issues.

AppArmor is happy to provide support for all FDLE end users and for the administrative staff from Monday-Friday 8:00 am to 6PM EST to assist with any issues with the system. The next question will identify the SLAs and escalation plan for all error and bug reporting.

3.4 - The Contractor should have a defined escalation plan for technical problems that cannot be resolved by the Help Desk. The escalation plan must include a definition of severity levels and specific escalation procedures based upon the severity of the technical problem.

See the AppArmor Support Plans and related SLAs table below for reference to subsequent questions:



AppArmor Support Plans

	Basic	Enhanced	Premium
Content Support			
Response Time	Week	1-2 days	1 day
Technical Support			
Business Critical	9-5/5 4 business hrs	95-/5 1 business hour	24/7, 365 1hr
Degraded Service	9-5/5, 2 business days	9-5/5, 1 business day	9.5/5 4 business hours
General Issue	4 busines days	2 business days	1 business day
Contact Available			
Email Support	Yes	Yes	Yes
Phone Support	No	9-5, 5 days a week	9-5/5, 5 days a week (Gen, Deg), 24/7 365 for business critical.
Video Training	Yes	Yes	Yes
Online Documentation	Yes	Yes	Yes

Definitions
Business Critical - Priority One
Represents a complete loss of service or a significant feature that is completely unavailable and no workaround exists. Does not include items that are in development or sandbox environments.
Degraded Service - Priority Two
Includes intermittent issues or reduced quality of service. A workaround may be available. Does not include development issues in development or sandbox environments.
General Issue - Priority Three
Includes product questions, feature requests, and all non-urgent support.

Observed Holidays	Date
New Year's Day	Jan 1 or Observed
Family Day	3rd Monday of February
Good Friday	Varies by year.
Victoria Day	Monday preceding May 25
Canada Day	Monday after Jul 1
Civic Holiday	First Monday in August
Labour Day	First Monday in September
Can. Thanksgiving	Second Monday in October
Christmas Day	25-Dec
Boxing Day	26-Dec

Only 24/7/365 support available on holidays.

Support related issues on the platform are divided into 3 categories:

Business Critical: Only available for production applications. Represents a complete loss of service or a significant feature that is completely unavailable, and no workaround exists. Does not include development issues or problems in staging environments.

Degraded Service: Includes intermittent issues and reduced quality of service. A workaround may be available. Does not include development issues or problems in staging environments.

General Issue: Includes product questions, feature requests and development issues.

In all cases, the State and FDLE is made aware of the issue if AppArmor discovers it prior to the institution. Further, our systems are constantly automatically monitored; any error messages create an automatic support ticket which will be processed by our support team based on the criteria above; we call this "Proactive Persistent Support".

Business Critical and Degraded Service issues are automatically escalated to the most senior available support manager. General issues are handled on a case by case basis and are only escalated if additional expertise is needed to achieve a resolution.

For all non-urgent situations, AppArmor advises the partner institution to watch the readily available support videos and review any print material initially. In the instance the support issue persists, the partner institution can choose between an online support ticket via AppArmor dashboard or an email to the customer support team.

High quality customer service is a pillar of our business.

3.5 - The Contractor agrees to share with FDLE their road map for future development and enhancements of the system.

AppArmor views every engagement as a partnership with the organization. This means that our roadmap is very much influenced by suggestions and feedback from our customers. We would both expect and invite this same sort of arrangement with FDLE. To that end, we would be more than happy to share our road map of future enhancements with the State to better improve our platform.

4 - SERVICE LEVEL AGREEMENT

4.1 - System Availability: Minimum of 99.5% uptime, 24 hours a day, 7 days a week, and 365 days a year.

As has been stated throughout this response, our uptime SLAs is 99.95%, 24 hours a day, 7 days a week, 365 days a year. This is true for both the mobile app, webpage, and dashboard components of the platform.

4.2 - System Recovery Time Objective (RTO) - One (1) hour

AppArmor agrees to a system recovery time objective of 1 hour.

4.3 - System Recovery Point Objective (RPO) - Thirty (30) minutes

AppArmor agrees to a system recovery point objective of 30 minutes.

4.4 - Incident Severity Levels and Response Times

Business Critical: Only available for production applications. Represents a complete loss of service or a significant feature that is completely unavailable, and no workaround exists. Does not include development issues or problems in staging environments. **Maximum** response time: 1 hour

Degraded Service: Includes intermittent issues and reduced quality of service. A workaround may be available. Does not include development issues or problems in staging environments. **Maximum** response time: 4 hours

General Issue: Includes product questions, feature requests and development issues. **Maximum** response time: 1 business day.

4.5 - The Contractor should notify FDLE at least two (2) work days prior to planned system downtime. FDLE will specify the contacts and method of notification.

In terms of requirements on the client or downtime; there is no downtime for updates. AppArmor uses the DevOps “Continuous Delivery” Approach, meaning that redundant systems are "slotted" allowing for no downtime. Updates are small, as to avoid major system changes which could cause equally large issues or user confusion.

At AppArmor, we create new capabilities on our development server, test them on development and staging servers, and then when approved by our team, deploy to the production dashboard. We would communicate the change to your team prior to deployment and include training resources as necessary.

The AppArmor development team rigorously tests all new features, content, systems and anything pertaining to a new update. AppArmor has multiple servers and staging environments that enable the development team to test for numerous variables to ensure the new update has no compatibility issues. This would be done significantly before any update took place.

AppArmor is happy to discuss the potential updates and their affect with the State's IT team and any other key stakeholders to ensure any update is accomplished without compatibility issues prior to the update’s launch.

If updates do require training on new features, AppArmor will ensure that all print manuals, video documentation are also updated and provided to the State significantly before the updates occur. Furthermore, personal training can be accomplished via webinar.

Lastly, as a step in the onboarding process, organizations are given the option to add additional items to the roadmap of releases. Otherwise, the release schedule is identified in the project management platform or online dashboard.

4.6 - All changes to the system, such as scheduled maintenance, should be announced to FDLE (2)work days prior to planned implementation and should be applied during non-peakhours (8 PM to 7 AM ET).

As the previous answer suggested, there is no downtime to the system. AppArmor uses the DevOps “Continuous Delivery” Approach, meaning that redundant systems are "slotted" allowing for no downtime. Updates are small, as to avoid major system changes which could cause equally large issues or user confusion.

AppArmor will however communicate any major changes that may affect usage of the system either by end users or FDLE staff.

TAB 5 – PUBLIC AWARENESS AND TRAINING

Below we've responded to the appropriate Functional Requirements per the ITN, Attachment F Section II, part C4.

1 - PUBLIC AWARENESS AND TRAINING

1.1 - The Contractor should provide a Public Awareness and Training Plan.

At all partner organizations, AppArmor provides a "Marketing Launch Toolkit" which includes:

1. A marketing plan to market the solution based on historical best practices
2. A one-minute video featuring the platform (which is closed captioned)
3. Screenshots of the app on iOS and Android devices
4. Screenshots of the reporting webpage on Macintosh and Windows devices
5. Business Card Sized Handouts
6. Sample Posters
7. Sample Social Media Posts

Additional items are available upon request by the State. Further, we are happy to engage with State marketing personnel to develop a detailed marketing strategy.

An important note here is that AppArmor apps generally speaking see 50-100 times more downloads versus other equivalent apps in the market. This is due to the custom branded "white labelled" aspect of the platform which is a pillar of our business.

As for training on the system; it is extremely important for the successful deployment of the safety app with advanced reporting with FDLE. We provide significant training, in the form of remote training sessions (webinars) when necessary, and significant video training and documentation.

Like FDLE, AppArmor is extremely interested in ensuring that your staff members are not just trained, but experts of the platform. We provided unlimited training sessions and we are available 24/7/365 for additional questions and support as required. We view every project we take on us a partnership; we want to be there for you should you have a question.

The training period can run from a single hour session to multi-day on site visits. However, given the large number of agencies across significant geographical areas, we believe webinars are the most efficient route.

Further, ongoing training is provided at no additional cost to FDLE staff. Simply schedule it with our team. We also want to ensure that there is a high level of comfort using our software.

Additional Details: The following types of training are available:

1. Webinar based training with an online instructor – conducted via "GoTo Meeting", staff can be taken through a detailed training session that ends with them sending a mass notification to a test group.
2. Online self-help via documentation and video documentation. – We have a significant video and document library
3. On-site training – On-site training of the system which discusses the history and usage of the system.

1.2 - The Contractor should provide training services regarding use of the system to school staff, administrators and law enforcement personnel.

As noted in the previous question, we take training very seriously. We provide significant training, in the form of remote training sessions (webinars) and significant video training and documentation.

Like FDLE, AppArmor is extremely interested in ensuring that your staff members are not just trained, but experts of the platform. We provided unlimited training sessions and we are available 24/7/365 for additional questions and support as required. We view every project we take on us a partnership; we want to be there for you should you have a question.

The training period can run from a single hour session to multi-day on site visits. However, given the large number of agencies across significant geographical areas, we believe webinars are the most efficient route.

1.3 - The Contractor should provide public awareness services and materials to schools.

As noted in the first answer of this Tab, AppArmor will provide a "Marketing Launch Toolkit" which includes:

1. A marketing plan to market the solution based on historical best practices
2. A one-minute video featuring the platform (which is closed captioned)
3. Screenshots of the app on iOS and Android devices
4. Screenshots of the reporting webpage on Macintosh and Windows devices
5. Business Card Sized Handouts
6. Sample Posters
7. Sample Social Media Posts

Additional items are available upon request by the State. Further, we are happy to engage with State marketing personnel to develop a detailed marketing strategy.

1.4 - The Contractor should work with the State in the development and delivery of the training and awareness programs.

AppArmor is readily available to "train the trainer" or provide any services necessary to the State to ensure the successful deployment of the system. We are also happy to comment and work collaboratively on a general strategy to ensure the successful training of a broad range of FDLE staff.

1.5 - The Contractor will produce and deliver written and online/webinar trainings and training materials for school staff, administrators and law enforcement personnel.

Absolutely. AppArmor will provide previous recordings of all webinars which will be available for all years that FDLE is on the system, as well as video documentation on usage of the system and written documentation outlining its features. This information will be available for dissemination to school staff, administration and law enforcement personnel.

Again, AppArmor takes training very seriously; we will not rest until the State feels comfortable in using the software.

TAB 6 – OPTIONAL COMMODITIES AND SERVICES

The AppArmor Safety app platform has over 50 features. Below we've identified additional capabilities that the State could optionally add to its app at no additional cost.

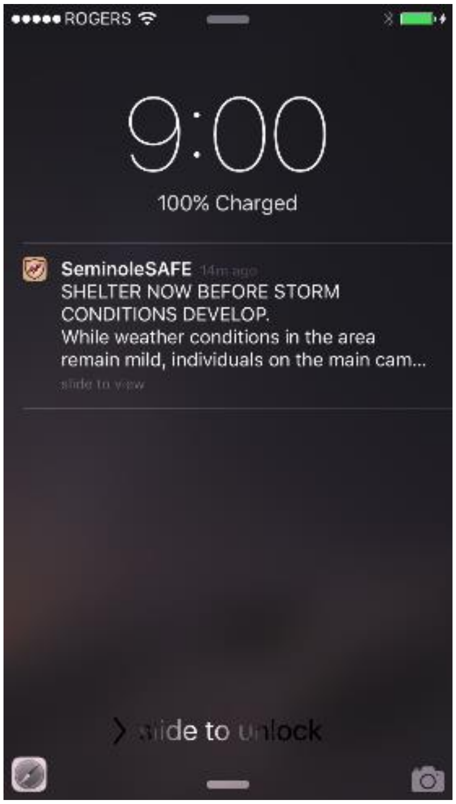
Ability for Push Notifications and Push Notification Channels

All of our apps come with unlimited push notifications. This means that The State and FDLE can send an unlimited number of push notifications to an unlimited number of users an unlimited number of times; there is no limit or cost per message sent.

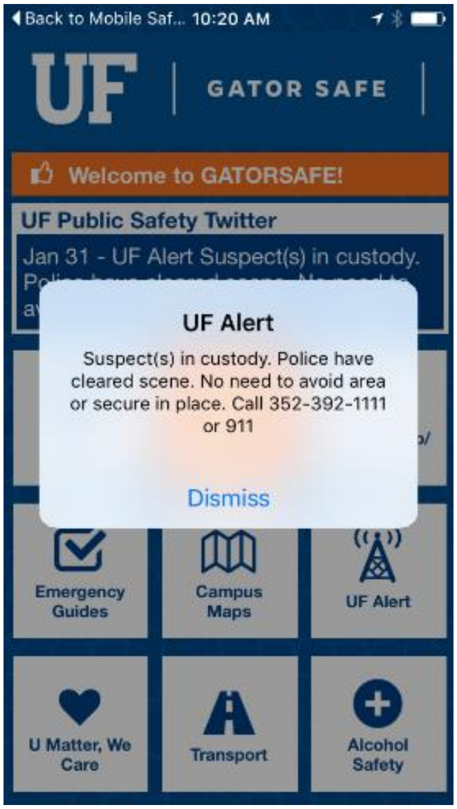
Some important considerations for push notifications versus other forms of mass notifications (such as Mass SMS messages):

1. Messages travel over Wi-Fi and cellular so they reach more end users (such as those not on cell)
2. Push notification delivery times are within 1-5 seconds for the entire payload, versus several minutes for SMS.
3. Push notifications drive users into their safety app (even when it's not previously running) to give the end user timely relevant and accurate information in a crisis.

Below are some screenshots from actual push notifications on other apps on the AppArmor platform:



SeminoleSAFE 14m ago
SHELTER NOW BEFORE STORM CONDITIONS DEVELOP.
While weather conditions in the area remain mild, individuals on the main cam...



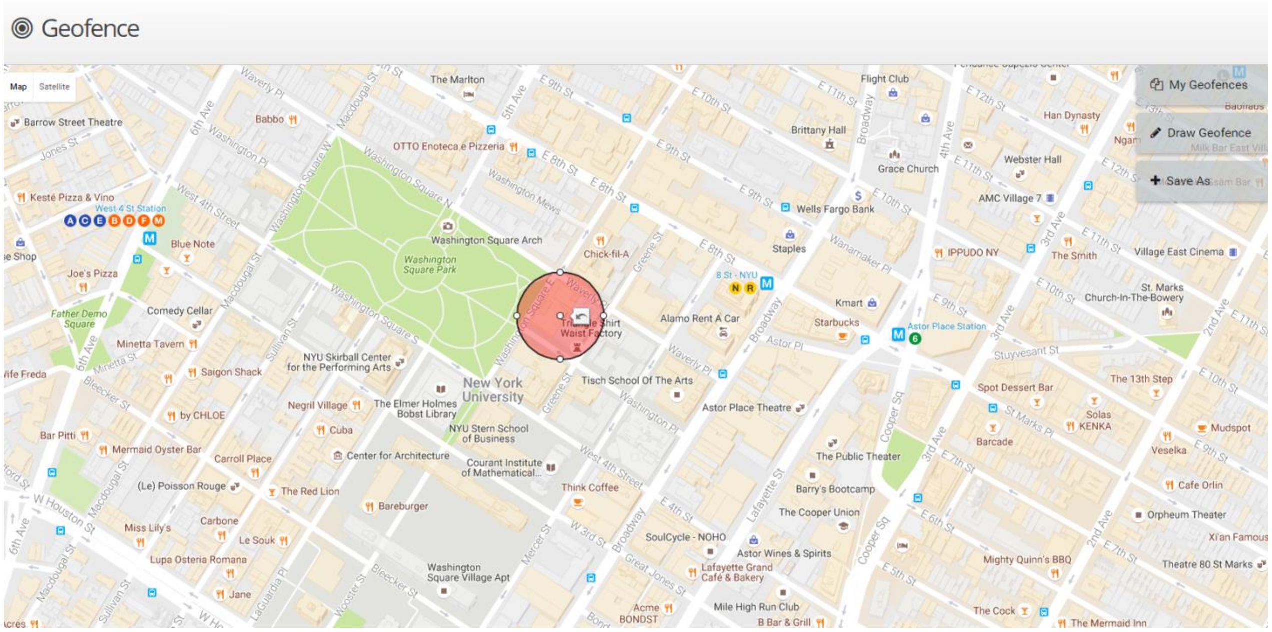
UF Public Safety Twitter
Jan 31 - UF Alert Suspect(s) in custody.

UF Alert

Suspect(s) in custody. Police have cleared scene. No need to avoid area or secure in place. Call 352-392-1111 or 911

AppArmor is also happy to provide unlimited "push notification channels". The channels segment the entire group of push notification users into specific categories, such as "exchange students" or even based on alert, i.e. "emergency alerts". This way, the right user gets the right message. Below is an example on another institution's app (next page):

Further, AppArmor is also happy to provide unlimited geo-located push notifications. Authorized officials at The State and FDLE are able to send a push to a certain area of the world and the message will be delivered to the users who have the app running in that area. Below is an example of that in the standard "circle" format from the perspective of the individual sending the mass notification:

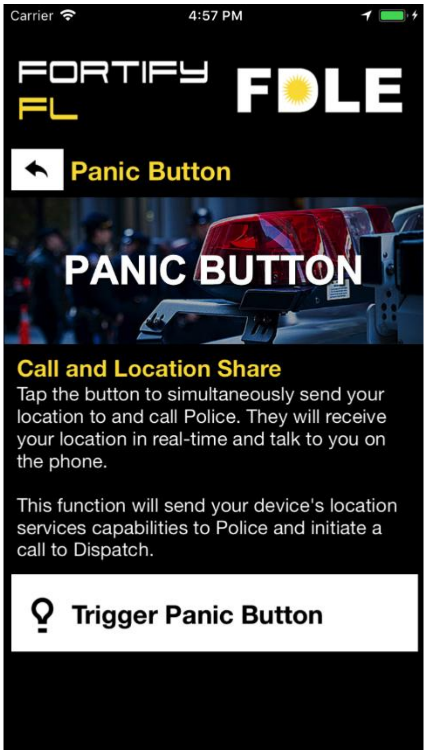


In all, AppArmor can provide numerous forms of push notifications which have particular advantages and are limited only by restrictions enforced by mobile operating systems (which all app developers must adhere to). We would work carefully with The State and FDLE to determine how to best configure the app in the context of push notifications.

Provide GPS location of callers or texters to dispatch upon call or text

This is a functionality that we've provided to the majority of the partner institutions on the AppArmor platform. Some institutions have opted out for resourcing reasons but this is essentially a primary function of the platform. We've outlined the process below in the context of a call to dispatch. However, the experience would be similar for a text message. A video on this can also be found here: https://youtu.be/Q0HFcNKzJu4 .

Step 1: The end user triggers the emergency call (Mobile BlueLight in this case although it can be branded to whatever The State and FDLE would prefer) via the app:



Panic Button

PANIC BUTTON

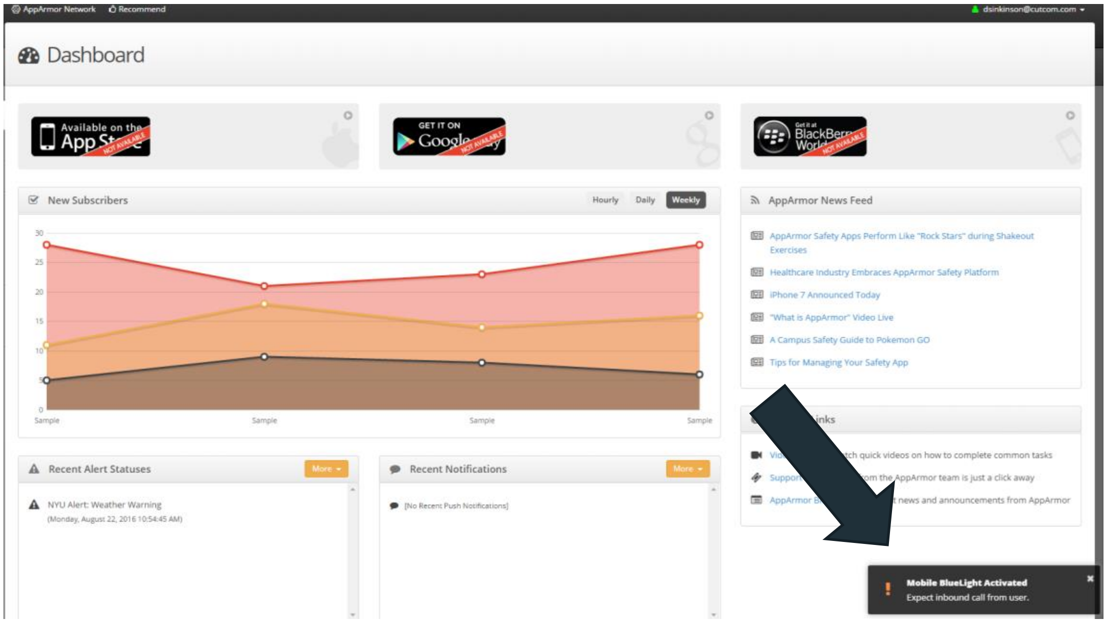
Call and Location Share

Tap the button to simultaneously send your location to and call Police. They will receive your location in real-time and talk to you on the phone.

This function will send your device's location services capabilities to Police and initiate a call to Dispatch.

Trigger Panic Button

Step 2: The dispatcher, who has the cloud based dashboard open (it can be on any device and never "times out") receives a notification in the bottom right corner of the screen. An alarm noise is also triggered and the dashboard's computerized voice says "Incoming Mobile BlueLight Alert" ensuring the dispatcher is aware of the emergency. (continued on next page)



AppArmor Safety Apps Perform Like "Rock Stars" during Shakeout Exercises

Healthcare Industry Embraces AppArmor Safety Platform

iPhone 7 Announced Today

"What is AppArmor" Video Live

A Campus Safety Guide to Pokemon GO

Tips for Managing Your Safety App

Vid tch quick videos on how to complete common tasks

Suppor om the AppArmor team is just a click away

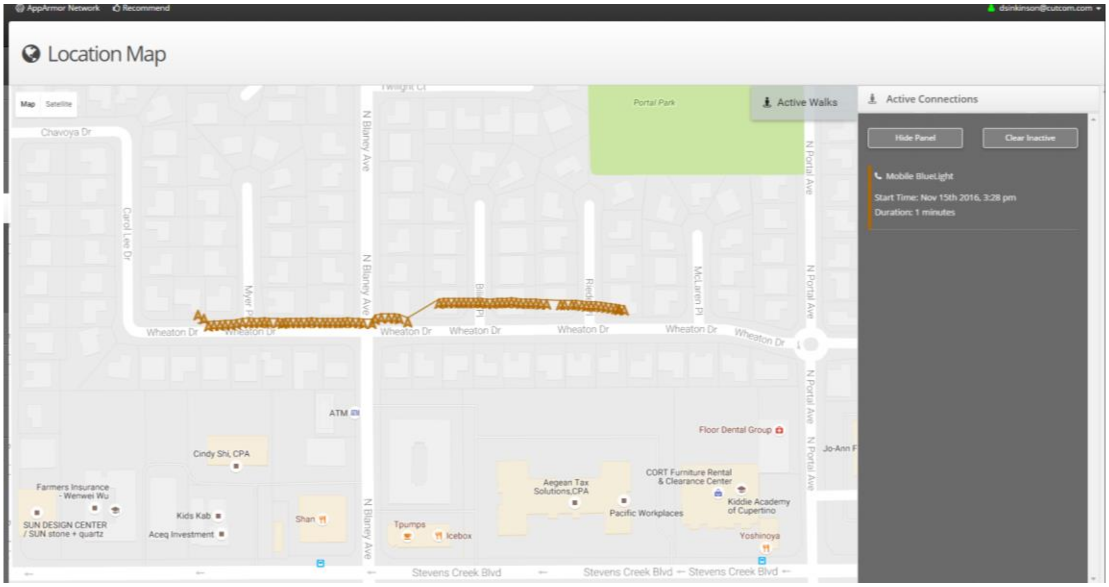
AppArmor B t news and announcements from AppArmor

NYU Alert: Weather Warning
(Monday, August 22, 2016 10:54:45 AM)

[No Recent Push Notifications]

Mobile BlueLight Activated
Expect inbound call from user.

Step 3: The dispatcher then simultaneously receives a phone call from and the location of the user. The dispatcher has the option to refuse the alarm (thereby not tracking) should they desire. Should the dispatcher not refuse, they are taken to the location map where they can see the user's location in real time.

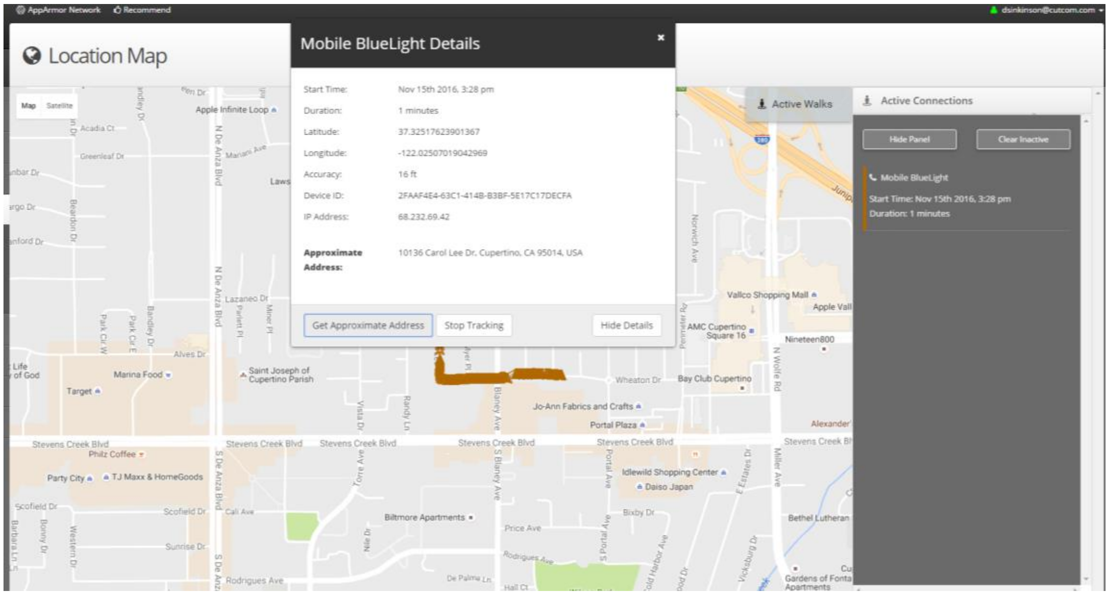


Mobile BlueLight

Start Time: Nov 15th 2016, 3:28 pm

Duration: 1 minutes

Step 4: The dispatcher watches the user while talking to them. They also rally an emergency response.



Mobile BlueLight Details

Start Time: Nov 15th 2016, 3:28 pm

Duration: 1 minutes

Latitude: 37.32517623901367

Longitude: -122.02507019042969

Accuracy: 16 ft

Device ID: 2FAAF4E4-63C1-414B-B3BF-5E17C17DECFA

IP Address: 68.232.69.42

Approximate Address: 10136 Carol Lee Dr, Cupertino, CA 95014, USA

Mobile BlueLight

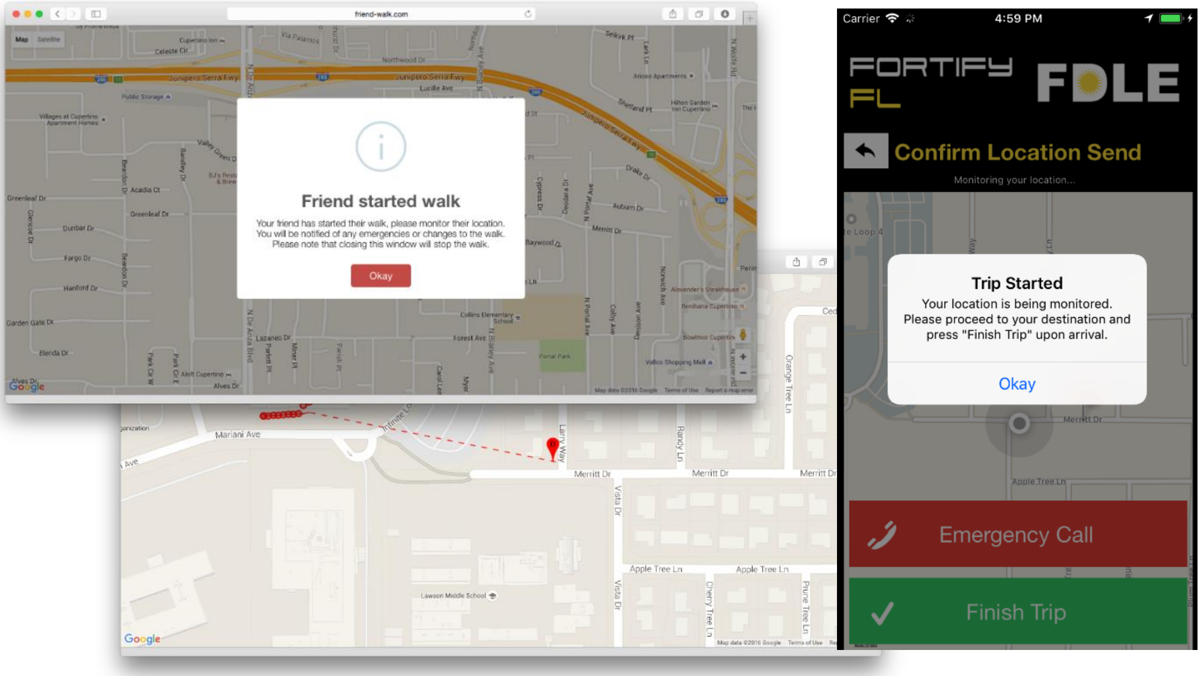
Start Time: Nov 15th 2016, 3:28 pm

Duration: 1 minutes

Step 5: The dispatcher can pull up additional details on the user as necessary. Note that with Single Sign On integration, more details on the user would be available. A history of all panics is available in the online dashboard.

Friend Walk/Send Location to a Contact tracking capability

AppArmor's platform also includes "Friend Walk" a feature where the user can send their location to a contact in their phone so they monitor their progress across campus/community. The "Friend" does not have to have the application (making this feature more accessible) and the user is warned if they "Friend" navigates away from the monitoring webpage. This is a very popular feature of the platform.



Friend started walk

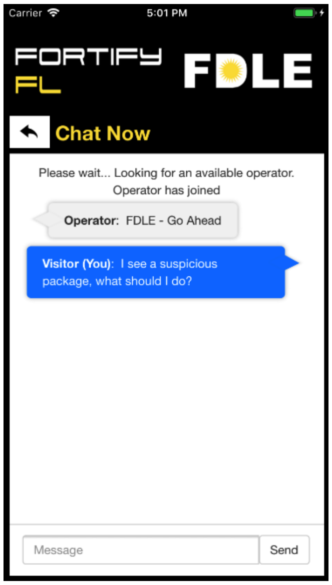
Your friend has started their walk, please monitor their location. You will be notified of any emergencies or changes to the walk. Please note that closing this window will stop the walk.

Trip Started

Your location is being monitored. Please proceed to your destination and press "Finish Trip" upon arrival.

f. 2-Way Administrative Dashboard to Interact with App Users

Our dashboard can interact with user in 2-way communications in form of our chat feature. The experience is fairly straightforward: the user opens the app, selects the chat function. They are then connected to the dispatcher in real time. Below are screenshots:

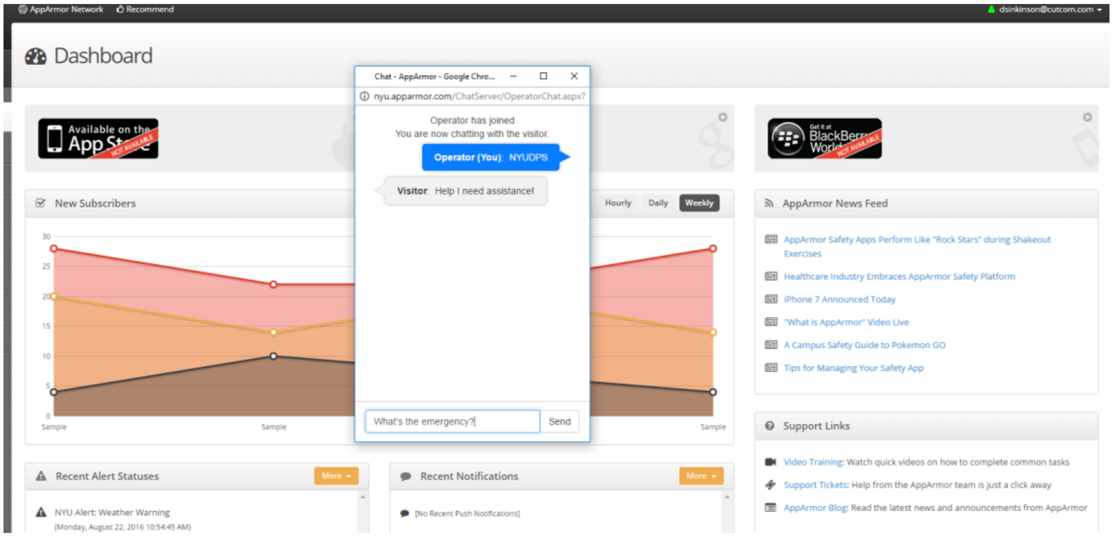


Please wait... Looking for an available operator.
Operator has joined

Operator: FDLE - Go Ahead

Visitor (You): I see a suspicious package, what should I do?

The dispatcher is able to have multiple chats going simultaneously as they "pop out" as additional browser windows from the cloud dashboard. See image below.



Operator has joined
You are now chatting with the visitor.

Operator (You): NYUDPS

Visitor: Help I need assistance!

What's the emergency?

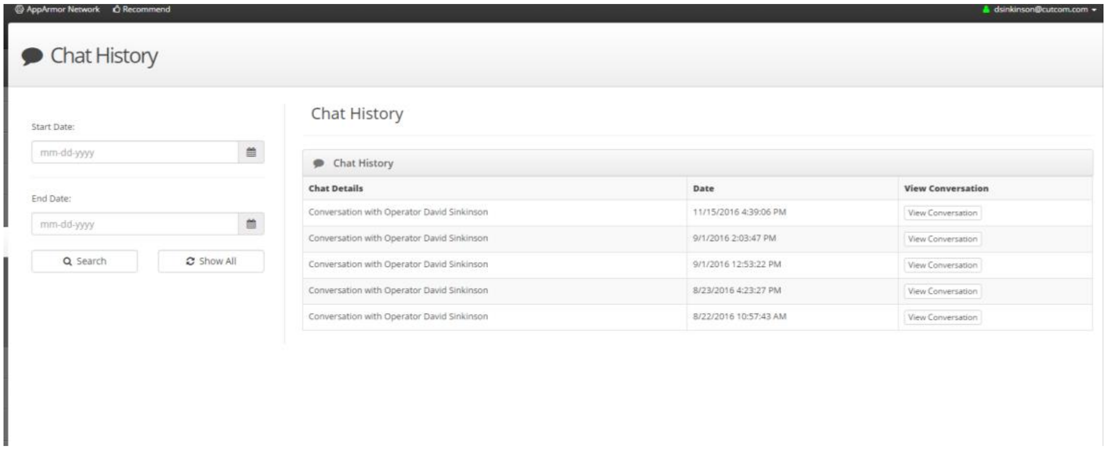
NYU Alert: Weather Warning
(Monday, August 22, 2016 10:54:45 AM)

[No Recent Push Notifications]

- AppArmor Safety Apps Perform Like "Rock Stars" during Shakeout Exercises
- Healthcare Industry Embraces AppArmor Safety Platform
- iPhone 7 Announced Today
- "What is AppArmor" Video Live
- A Campus Safety Guide to Pokemon GO
- Tips for Managing Your Safety App

- Video Training: Watch quick videos on how to complete common tasks
- Support Tickets: Help from the AppArmor team is just a click away
- AppArmor Blog: Read the latest news and announcements from AppArmor

All chats are stored in the "Chat History" in the online dashboard (pictured below). Note that chats can be anonymous or detailed with the user information from the single sign on integration.



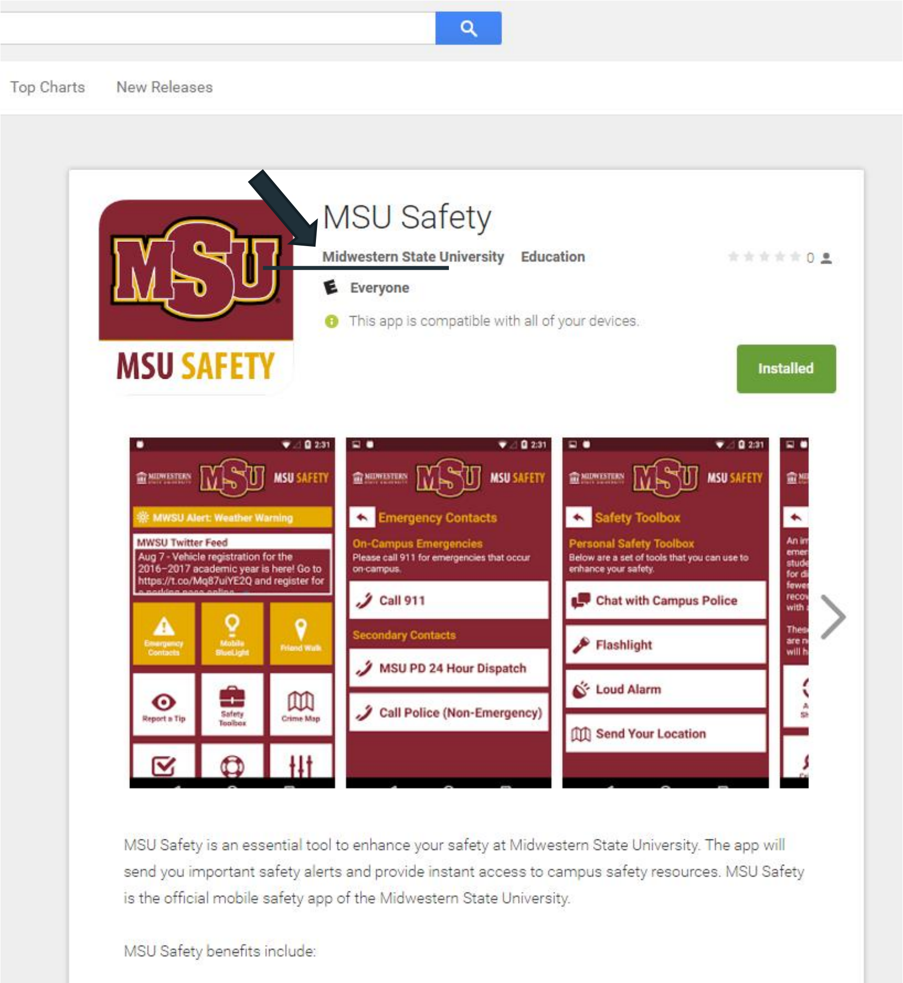
Chat History

Chat History

Chat Details	Date	View Conversation
Conversation with Operator David Sinkinson	11/15/2016 4:39:06 PM	View Conversation
Conversation with Operator David Sinkinson	9/1/2016 2:03:47 PM	View Conversation
Conversation with Operator David Sinkinson	9/1/2016 12:53:22 PM	View Conversation
Conversation with Operator David Sinkinson	8/23/2016 4:23:27 PM	View Conversation
Conversation with Operator David Sinkinson	8/22/2016 10:57:43 AM	View Conversation

The State and FDLE own the data of the app users

All AppArmor custom mobile safety apps are deployed under the app store accounts of the partner organization. Among the many other benefits of AppArmor safety apps, this is a distinct advantage that other vendors will be unlikely to offer you (as they tend to submit their apps under their app store accounts). The importance of this unique benefit is that you control the user base and all user data exclusively. Also, it gives you enhanced flexibility should you wish to replace any vendor as all that's required is an app update. If you were to pick another vendor and want to switch to another provider later, you would lose all your downloads (user base) for the app. Here's an example at Midwestern State University in Texas:



This app is compatible with all of your devices.

MSU Safety is an essential tool to enhance your safety at Midwestern State University. The app will send you important safety alerts and provide instant access to campus safety resources. MSU Safety is the official mobile safety app of the Midwestern State University.

MSU Safety benefits include:

All information used in the app is the property of The State and FDLE. AppArmor is the provider of a platform for custom mobile app development and configuration and does not own the content whatsoever. AppArmor does not own any personal or non-personal information of users or content as it pertains to the app.

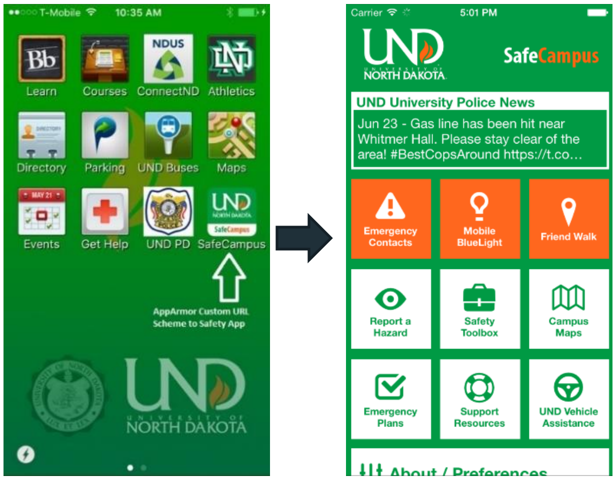
The app is submitted under the App store accounts of the institution

Further to the previous section, we believe that it's very important that the institution retains ownership over the app user base and has flexibility in how it deploys its safety app. To that end, every AppArmor app is submitted under the App Store accounts of the institution. We believe this is not only a huge benefit of our approach (as it guarantees higher downloads for the institution) but it also consistent with our philosophy of developing a partnership with our customers.

Custom URL Schemes and Links to Other Institutional Apps as Designated

Our platform uses "Custom URL Schemes" to make it possible for our app to be opened from another application and vice versa. This same technology will work for other apps that the State and FDLE deem relevant. This is simply the best way to connect to completely separate apps. Otherwise though, hyperlinks and browser windows can be utilized instead of a custom URL scheme to highlight another application.

This is a Custom URL Scheme from The University of North Dakota App and their safety app from AppArmor, Safe Campus:



UND University Police News

Jun 23 - Gas line has been hit near Whitmer Hall. Please stay clear of the area! #BestCopsAround https://t.co…

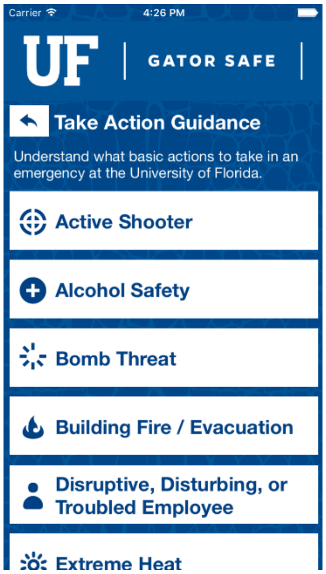
Note that the safety app can be opened from the institutional app. There is also a button in the SafeCampus app to open up the institutional app.

Florida State uses custom URL schemes to connect its app to WAZE, other FSU apps, and much more. Many institutions are excited about this new capability in mobile applications and we're happy to provide it to The State and FDLE.

Ability to Share offline ready Pre-Stored Preparedness Plans Within the App for User Review

This another important distinction of the AppArmor safety app platform versus other in-market solutions. All AppArmor apps are "native" mobile apps meaning that unlike "hybrid" apps or "mobile sites", our native mobile apps can store content offline. As a result, if a user was without a data connection (cellular or Wi-Fi) they would still be able to access app content (note: other features which require a data connection, such as calling functions, would not work).

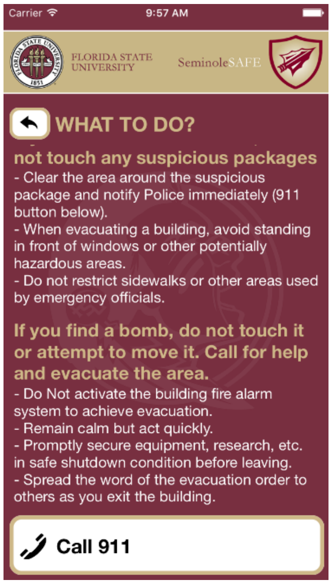
If the user *is* connected to a data connection, then we make the emergency plans more actionable by providing buttons/features which can execute what the preparedness plans suggest. For instance, see the images below. From left to right, the first image shows offline content and the second image shows the added functionality for emergency plans:



Take Action Guidance

Understand what basic actions to take in an emergency at the University of Florida.

- Active Shooter
- Alcohol Safety
- Bomb Threat
- Building Fire / Evacuation
- Disruptive, Disturbing, or Troubled Employee
- Extreme Heat



WHAT TO DO?

not touch any suspicious packages

- Clear the area around the suspicious package and notify Police immediately (911 button below).
- When evacuating a building, avoid standing in front of windows or other potentially hazardous areas.
- Do not restrict sidewalks or other areas used by emergency officials.

If you find a bomb, do not touch it or attempt to move it. Call for help and evacuate the area.

- Do Not activate the building fire alarm system to achieve evacuation.
- Remain calm but act quickly.
- Promptly secure equipment, research, etc. in safe shutdown condition before leaving.
- Spread the word of the evacuation order to others as you exit the building.

All this content would be set by The State and FDLE. And all of the content can be modified in real time via the online cloud based dashboard.

Support Single Sign On

AppArmor has integrated at other organizations various forms of single sign on support. For The State and FDLE, we would accommodate this request should it be necessary. For more detailed technical instructions on the nature of the integration, we would need documentation from The State and FDLE IT. The dashboard or app will however request a set of credentials (likely some sort of The State and FDLE ID or The State and FDLE email address and password) at initial login. After first time login, the user will not be required to login again. Additional options can be set by The State and FDLE, such as a mandatory re-authentication after 30 days of being signed in.

Additional Mass Notification Options for the System

Via the AppArmor Alert System, the State would have access to (at an additional cost) the following mass notification options all of which would be aggregated in the AppArmor dashboard:

1. Mass Push Notifications
2. Mass SMS (Text) Messages
3. Mass Email
4. Mass Outbound Calling
5. Desktop Notifications (with optional panic button)
6. RSS/ATOM/CAP XML/ Http Activation Feeds
7. Social Media Broadcasting

SOFTWARE CONFIGURATION AND SUPPORT AGREEMENT

THIS SOFTWARE CONFIGURATION AND SUPPORT AGREEMENT (the "Agreement") dated as of August 1st 2018 (the "Effective Date")

BETWEEN:

(1) Cutcom Software Inc., DBA AppArmor, a company incorporated in the Province of Ontario and having its principal place of business at 545 King Street West, Toronto, Ontario, Canada ("AppArmor"); and

(2) The Florida Department of Law Enforcement, having its principal place of business at 2331 Phillips Rd, Tallahassee, FL 32308, USA (the "Customer")

WHEREAS the Customer requires software configuration and ongoing support services for a mobile safety application for smartphones (running various operating systems) for use by the Customer and end-users affiliated with the Customer;

AND WHEREAS AppArmor is prepared to provide these software configuration and support services to the Customer according to the terms of this Agreement;

THE PARTIES AGREE as follows:

1 **The Services.** AppArmor agrees to provide to the Customer the "Configuration Services" and the "Support Services" as described in Section 1(a) and Section 1(b) of this Agreement (together, the "Services").

(a) Configuration Services

(i) AppArmor will configure the customized mobile safety application (the "App") in accordance with the specifications set out in Schedule "A". For greater certainty, the specific steps that AppArmor will take in order to configure the App are set out in Schedule "B".

(ii) AppArmor will make the App available for public download on or before August 15th 2018 (the "Availability Date").

(iii) AppArmor will make the App available for public download on one or more of the following distribution platforms as agreed upon by AppArmor and the Customer: the AppStore, a digital distribution service for mobile apps on iOS devices operated by Apple, Inc. ("the App Store"); Google Play, a digital distribution service for mobile apps on Android operating system devices operated by Google, Inc. ("Google Play"); or any other distribution service mutually agreed upon by AppArmor and the Customer (collectively, the "Distribution Platforms").

(b) Support Services

(i) Beginning on the Availability Date and continuing for the duration of the Term (as defined in Section 2) of this Agreement, AppArmor will maintain the App in substantial conformity with the specifications set out in Schedule "A", and will provide further services as described in Schedule "C".

(ii) The Support Services do not require AppArmor to repair or correct bugs or operational issues in the App brought about by third party software or hardware. If the Customer wants AppArmor to repair or correct the App as a result of bugs or operational issues in the App brought about by third party software or hardware, additional fees may apply subject to agreement by the parties. The repairs and corrections provided by AppArmor to the Customer will be considered part of the App and subject to the terms and conditions of this Agreement, or such agreement, if any, which accompanies such repairs and corrections.

(iii) Any derivative works of the App created by or for AppArmor from time to time and all copies of the App including translations, compilations, and partial copies, and the media on which any of the foregoing are stored or printed are, and at all times continue to remain, the property of AppArmor, and the Customer forever disclaims any rights of ownership therein, including any intellectual property rights.

(iv) If the Customer requests modifications to the App other than those described in Schedule "C", AppArmor will prepare a proposal identifying or describing the additional work, services or changes to be performed, an estimate of the amount or rates AppArmor will charge to perform the work, services or changes and a revised schedule of performance for the requested changes ("Project Impact Proposal" or "PIP"). Upon receipt of a signed amendment or work order from the Customer to pay the charges for the requested changes, AppArmor agrees to perform the additional work, service, or changes identified in the PIP.

2 Term.

(a) This Agreement is effective between the Customer and AppArmor as of the Effective Date.

(b) The "Effective Date" and "Initial Term" of this agreement as well as all renewals is governed by the attached document "Florida Department of Law Enforcement Contract FDLE-005-19"

3 Payment.

(a) The Payment terms are governed by the attached document "Florida Department of Law Enforcement Contract FDLE-005-19"

(b) Unless otherwise indicated, all amounts in this Agreement are stated and are payable in United States dollars.

4 Third Party Fees.

(a) Any fees payable by the Customer to third parties ("Third Party Fees"), including any fees related to the App's submission to any Distribution Platform, shall be paid by the Customer. At the time of this agreement these fees are $99.00 annually to Apple, and $25.00 one time to Google.

(b) AppArmor shall not be responsible for any Third Party Fees.

5 Termination.

(a) Termination of this agreement is governed by the attached document "Florida Department of Law Enforcement Contract FDLE-005-19".

6 **Customer Trademark Licenses.**

(a) During the Term, the Customer grants to AppArmor a non-assignable, non-exclusive, royalty-free, worldwide license to use and display publicly the trademarks the Customer provides to AppArmor to include in the App.

(b) During the Term and conditional upon AppArmor's receipt of written permission from the Customer, the Customer grants to AppArmor a non-assignable, non-exclusive, royalty-free, worldwide license to use and display publicly the trademarks the Customer provides to AppArmor to include in the Marketing Toolkit described in Schedule "B". AppArmor acknowledges that it shall not use Customer's name, logo(s), trademark(s), or any other identifying marks or symbols for any promotional purpose which is not expressly provided for in the scope of work without the written consent of FDLE.

(c) AppArmor acknowledges that it has not acquired, and will not acquire, any ownership rights in the Customer's trademarks.

(d) The Customer reserves the right to inspect AppArmor's use or display of the Customer's trademarks.

7 **Ownership of Intellectual Property.**

(a) Subject to Section 6, Section 7(e) and any software that AppArmor properly licences from third parties, AppArmor shall be the exclusive owner of the App and the Marketing Toolkit and of all intellectual property rights in and to the App and the Marketing Toolkit.

(b) Subject to Section 6 and Section 7(e), the Customer hereby assigns all right, title and interest throughout the world, including without limitation, all copyrights, trademarks, trade secrets, patent rights, and any other intellectual property rights in and to the App and the Marketing Toolkit, effective at the time each is created.

(c) The Customer agrees that it shall not, either during the Term of this Agreement or thereafter, directly or indirectly, contest, or assist any third party to contest, AppArmor's ownership of the App and the Marketing Toolkit and any intellectual property rights related thereto.

(d) The Customer acknowledges and agrees that the rights granted to it under this Agreement shall not in any way prevent or preclude AppArmor, or in any way be deemed to prevent or preclude AppArmor, from licensing software that makes up the App and using the Marketing Toolkit, AppArmor's knowledge, experience, know-how, and expertise to perform work for others which result in the creation of software, works, and related materials having formats, organization, structure, and sequence similar to the work originated and prepared for the Customer.

(e) Notwithstanding any other provisions in this Section 7, the Customer shall retain any intellectual property in any materials that it provides to AppArmor to be included as content in the App.

(f) The Customer's use of the App is governed by the end-user licence agreement that the Customer enters into with Google and Apple via the Google Play and AppStore.

8 **Reverse Engineering.**

(a) The Customer agrees that it will not: (i) decompile, disassemble, or otherwise reverse engineer any of the App or knowingly contribute to the decompilation, disassembly, or reverse engineering by a third party; or (ii) modify or create any derivative work of the App.

9 Feedback.

(a) The Customer agrees that AppArmor shall own all feedback, ideas, concepts, or changes to the App identified, suggested, or provided to AppArmor by the Customer and all associated intellectual property rights (collectively the "Feedback"), and hereby assigns to AppArmor all of its right, title, and interest thereto.

(b) The Customer agrees to cooperate fully and to ensure that its employees and all third parties, if applicable, cooperate fully with AppArmor, both during and after the termination of this Agreement and the applicable end-user license agreement with respect to signing further documents and doing such other acts as are reasonably requested by AppArmor to confirm its ownership in the Feedback, and to enable AppArmor to register or protect any intellectual property rights and/or Confidential Information (as defined in Section 10 of this Agreement) in the Feedback.

10 Confidentiality.

(a) The Customer shall not disclose any proprietary or confidential information related to the App or the Services (the "Confidential Information") that is disclosed to the Customer by AppArmor.

(b) Confidential Information includes all business, financial, technical, and other information marked or designated by AppArmor as "confidential" or "proprietary", as well as any information which, by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as confidential. Without limiting the generality of the foregoing, Confidential Information expressly includes any password-protected information that is made available to the Customer by AppArmor, including but not limited to information contained on the Online Dashboard described in Schedule "C".

(c) Any information or materials provided by AppArmor in relation to the App, together with any Feedback provided by the Customer, shall be deemed AppArmor's Confidential Information and the Customer shall comply with its confidentiality obligations in accordance with this Agreement.

(d) Confidential Information shall not include: information that is currently in the public domain or that enters the public domain by no fault of the Customer after the signing of this Agreement; information that the Customer lawfully receives from a third party without restriction on disclosure and without breach of a non-disclosure obligation; information that the Customer knew prior to receiving any Confidential Information from AppArmor; or information that the Customer independently develops without reliance on any Confidential Information from AppArmor. Excluded from the definition of "Confidential Information" is also any information which is disclosed pursuant to law, including, but not limited to, the State of Florida's public records laws.

(e) Without limiting the generality of the confidentiality obligations set out in this Section 10, or in any other way detracting from or limiting these obligations, the Customer shall be prohibited from using any AppArmor Confidential Information for the development of any technology, products, or services that compete with the technology, products, or services of AppArmor, and from enabling any third party to do any of these activities.

11 Indemnity.

(a) AppArmor shall indemnify, defend, and hold harmless the Customer from and against any and all claims, liabilities, damages, fines, causes of action, losses, and expenses (including, without limitation, lawyers' fees and expenses, expert witnesses' fees and expenses, costs of investigation and settlement, and court costs) to the extent they are caused or alleged to be caused by the gross negligence or intentional misconduct of AppArmor, any breach by AppArmor of any representation, warranty, or guarantee of AppArmor herein, any misappropriation of intellectual property of a third party by AppArmor, or by any claim that the App and Marketing Toolkit infringe a patent, trademark, copyright, or any intellectual property rights of a third party; *provided however*, that AppArmor shall have no liability, defense, or indemnification obligation to the extent the claim results from: (i) modification of the App or Marketing Toolkit made by anyone other than AppArmor; or (ii) the Customer's failure to use an updated or modified App or Marketing Toolkit provided by AppArmor, if a claim would have been avoided but for such failure to use such updated or modified App or Marketing Toolkit.

(b) If the Customer's use of the App and Marketing Toolkit hereunder is, or in AppArmor's opinion is likely to be, enjoined due to the type of claim specified in this Section 11(a), AppArmor may, at its sole option and expense: (i) procure for the Customer the right to continue using such App and Marketing Toolkit under the terms of this Agreement; (ii) replace or modify such App and Marketing Toolkit so that they are no longer infringing; or (iii) if options (i) and (ii) above cannot be accomplished despite AppArmor's reasonable efforts, then AppArmor may terminate the Customer's rights and AppArmor's obligations hereunder with respect to such App and Marketing Toolkit and refund unearned Support Fees, if any. The Customer shall promptly notify AppArmor in writing of any such claim, shall permit AppArmor to exercise sole control over the defense and settlement of such claim, and shall cooperate with AppArmor in the defense of the claim provided, however, AppArmor shall not settle any such claim without the prior written consent of the Customer, which shall not be unreasonably withheld or delayed.

12 Limitation of Liability.

(a) This section has been intentionally removed.

13 Relationship between Parties.

(a) AppArmor and the Customer are not legal partners or agents. Rather, the relationship between AppArmor and the Customer is that of independent contractors. For greater certainty, neither party shall have the authority to act on behalf of the other party or enter into any contracts, licences, or any other agreements on behalf of the other party.

(b) The Customer may, from time to time, grant access to AppArmor to its developer accounts for any Distribution Platforms. AppArmor agrees that it will act in accordance with all of the rules, regulations and agreements imposed by the Distribution Platforms in connection with such access. Where AppArmor wishes to exceed the limitations set forth in this Section 13(b), it shall first obtain the written permission of the Customer.

14 Miscellaneous

(a) No Waiver. No waiver by AppArmor or the Customer of a breach or omission under this Agreement shall be binding unless it is expressly made in writing and signed by the other party. A failure to enforce a provision of this Agreement is not a waiver of a party's right to do so later.

(b) Severance. If part of this Agreement is found to be unenforceable, the remaining parts of this Agreement will remain in full effect.

(c) Assignment. Assignment is governed by the attached document "Florida Department of Law Enforcement Contract FDLE-005-19"

(d) Force Majeure. Except for required payments, neither party shall be liable for failure to perform or for delay in performing its obligations to the extent and for so long as such failure or delay is due to fire, strike, lock-out, natural disasters, power failure, war, riots, acts of a civil or military authority, acts of God, judicial action, inability to secure necessary materials, or any causes reasonably beyond the control of such party. Any party desiring to invoke the protection of this Section 14(e) shall promptly notify the other party and use reasonable efforts to promptly resume performance of its obligations.

(e) Governing Law and Jurisdiction. This Agreement shall be governed by and construed under Florida law, with jurisdiction and venue lying in Leon County, Florida. Each party hereto irrevocably waives any objection on the grounds of venue, *forum nonconveniens* or any similar grounds and consents to the jurisdiction of the courts of the State of Florida, USA.

(f) Survival. Sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14 of this Agreement shall survive any termination or expiration of this Agreement.

(g) Notices. All notices and other communications required or permitted under this Agreement will be in writing and, except as otherwise provided in this Agreement, will be deemed given when delivered personally, sent by registered or certified mail, return receipt requested, sent by overnight courier to the address set out on the first page of this Agreement or to such other persons or places as AppArmor and the Customer may direct from time to time in accordance with this Section 14(h). Any notice shall be deemed to have been received when delivered, or, if mailed, shall be deemed to have been received four (4) business days after the date of mailing.

15 **Counterparts**. This Agreement may be signed in two or more counterparts each of which together will be deemed to be an original and all of which together will constitute one and the same instrument. Signing of this Agreement and transmission by facsimile or electronic document transfer will be acceptable and binding upon the parties hereto.

16 **Data Privacy**.

(a) AppArmor acknowledges and agrees that, in the course of its engagement by Customer, AppArmor may receive or have access to End User Personal Information. AppArmor shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such End User Personal Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of End User Personal Information under its control or in its possession by all authorized employees.

(b) End User Personal Information is deemed to be Confidential Information of Customer and is not Confidential Information of AppArmor. "End User Personal Information" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(c) In recognition of the foregoing, AppArmor agrees and covenants that it shall:

(i) keep and maintain all End User Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure;

(ii) use and disclose End User Personal Information solely and exclusively for the purposes for which the End User Personal Information, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available End User Personal Information for AppArmor's own purposes or for the benefit of anyone other than Customer, in each case, without Customer's prior written consent; and

(iii) not, directly or indirectly, disclose End User Personal Information to any person other than its authorized employees, without express written consent from Customer.

17 Data Security and Storage.

(a) AppArmor represents and warrants that its collection, access, use, storage, disposal and disclosure of End User Personal Information does and will comply with all applicable federal, state, and foreign privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Without limiting AppArmor's obligations under Section 16(a), AppArmor shall implement administrative, physical and technical safeguards to protect End User Personal Information, and shall ensure that all such safeguards, including the manner in which End User Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.

(c) At a minimum, AppArmor's safeguards for the protection of End User Personal Information shall include:

(i) limiting access of End User Personal Information to authorized employees;

(ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;

(iii) implementing network, device application, database and platform security;

(iv) securing information transmission, storage and disposal;

(v) implementing authentication and access controls within media, applications, operating systems and equipment;

(vi) encrypting End User Personal Information stored on any mobile media;

(vii) encrypting End User Personal Information transmitted over public or wireless networks;

(viii) strictly segregating End User Personal Information from information of AppArmor or its other customers so that End User Personal Information is not commingled with any other types of information;

(ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and

(x) providing appropriate privacy and information security training to AppArmor's employees.

(d) During the term of each authorized employee's employment by AppArmor, AppArmor shall at all times cause such authorized employees to abide strictly by AppArmor's obligations under this Agreement.

(e) Upon Customer's written request, AppArmor shall provide Customer with a network diagram that outlines AppArmor's information technology network infrastructure and all equipment used in relation to fulfilling of its obligations under this Agreement, including, without limitation:

(i) connectivity to Customer and all third parties who may access AppArmor's network to the extent the network contains End User Personal Information;

(ii) all network connections including remote access services and wireless connectivity;

(iii) all access control devices;

(iv) all back-up or redundant servers; and

(v) permitted access through each network connection.

18 **Return or Destruction of End User Personal Information.** At any time during the term of this Agreement at the Customer's written request or upon the termination or expiration of this Agreement for any reason, AppArmor shall, and shall instruct all Authorized Persons to, promptly return to the Customer all copies, whether in written, electronic or other form or media, of End User Personal Information in its possession or the possession of such Authorized Persons, or securely dispose of all such copies, and certify in writing to the Customer that such End User Personal Information has been returned to Customer or disposed of securely. AppArmor shall comply with all reasonable directions provided by Customer with respect to the return or disposal of End User Personal Information.

- Signature page follows -

The parties have had the opportunity to discuss this Agreement with their legal advisors.

IN WITNESS WHEREOF, each party hereto has caused this Agreement to be executed by its duly authorized representatives.

	CUTCOM SOFTWARE INC. (DBA APPARMOR)		The Florida Department of Law Enforcement
Signature:		Signature:	
Name:	David Sinkinson	Name:	Sonya Avant
Title:	Co-Founder	Title:	Chief of General Servies
Date:	July 30th 2018	Date:	07/31/2018

Attachments: Schedule "A", Schedule "B" and Schedule "C"

SCHEDULE "A"

APP AND WEBSITE SPECIFICATIONS

The App will consist of the following specifications:

a. Suspicious activity reporting capability by email, photo, or video;
b. Be Branded to the Customer as required
c. Other Specifications as determined by "Statement of Work FortifyFL"

Additionally, the App will optionally offer:

d. Emergency calling capability;
e. Push notification capability;
f. Mobile "BlueLight" emergency button with location share;
g. Friend walk location sharing with a contact;
h. Virtual walk-home location sharing with a dispatcher in the cloud dashboard;
i. Embedded information for health, counselling and disability services as requested;
j. Mapping capabilities including but not limited to a crime map;
k. "Geofencing" capabilities;
l. Additional Administrative dashboards as required;
m. Emergency plan documentation; and
n. Further customization based on standard feature set as determined by "Statement of Work FortifyFL"

The Website will consist of the following specifications

o. Suspicious activity reporting capability by email, photo, or video;
p. Be Branded to the Customer as required
q. Other Specifications as determined by "Statement of Work FortifyFL"

SCHEDULE "B"

STEPS TO CONFIGURE THE PLATFORM

The steps to configure the App and Website are as described below.

1 Distribution Platform Enrollments

In order for AppArmor to submit the App to a Distribution Platform, the Customer must enroll with the Distribution Platform to use their services. AppArmor will assist the Customer with the enrollment process.

2 Version 1 Design

AppArmor will customize the user interface of the App and Website to match the Customer's branding, content needs, and feature requests. AppArmor will seek the Customer's input, including review and feedback from the Customer's representatives. Once AppArmor receives permission from the Customer, it will proceed to the next step.

3 App Blueprint Design

AppArmor will work with the Customer to design the structure of the App and Website by creating a comprehensive blueprint (the "Blueprint"). The Blueprint provides a structure to the App by tailoring a combination of AppArmor modules to meet the needs of the end-users and the Customer.

4 Software Configuration

Once the Blueprint is complete, AppArmor will configure the software for the App and Website. This typically requires one (1) to two (2) weeks. AppArmor will provide on-going updates on its progress throughout the software configuration.

5 Testing

Once the software is configured, AppArmor will provide "beta" versions for the Customer's team to review and test to ensure the App meets the specifications set out in Schedule "A". The Customer agrees: (a) to test the App within three (3) days of receipt of the App; (b) to provide a verbal or written report on the progress of the testing and any bugs in the App; (c) to promptly retest the App within three (3) days of receipt of the corrected App; and (d) to promptly provide written acceptance of the App when it meets the specifications set out in Schedule "A". If the App meets the specifications set out in Schedule "A", the App will be deemed accepted by the Customer regardless if the Customer provides written acceptance. The Customer can provide Feedback to AppArmor, but if any of the Feedback requires development outside the scope of the specifications set out in Schedule "A", AppArmor is not obligated to do such development unless the parties agree otherwise and the Customer agrees to pay additional fees as agreed upon by the parties. If the Customer does not comply with the obligations set forth in this Section 5 and such failure results in an increase in the time required by AppArmor to perform any work, or affects AppArmor's ability to meet the Availability Date, or affects any other provision of this Agreement, AppArmor may extend the Availability Date and submit a written claim for an equitable adjustment to the payments required. The extension and claim shall be deemed to have been accepted unless the Customer notifies AppArmor of its basis for disagreement, in writing, within ten (10) days from the date of receipt of the notice of extension or claim.

6 App Store Submissions

The App will be submitted to one or more Distribution Platforms as mutually agreed by AppArmor and the Customer. AppArmor will use reasonable efforts to resolve any approval issues that may arise upon submission of the App to any Distribution Platform.

7 Marketing Assistance

AppArmor will provide the Customer with a "Marketing Toolkit" which includes:

(a) A suggested marketing strategy in a PowerPoint file for the launch of the App, including best practices and potential advertising channels;

(b) A suggested poster which features the App, left blank so the Customer can populate it with the Customer's chosen message;

(c) A suggested business card sized handout which features the App, left blank so the Customer can populate it with the Customer's chosen message;

(d) High resolution screenshot files of the App on devices running various operating systems; and

A short video meant to demonstrate the basic features of the App. The video may be broadcast on screens that the Customer may have and can be uploaded to

SCHEDULE "C"

SUPPORT SERVICES

In addition to maintaining the App in substantial conformity with the specifications set out in Schedule "A", the Support Services described in Section 1(b) will consist of the following services.

1 End-User Support

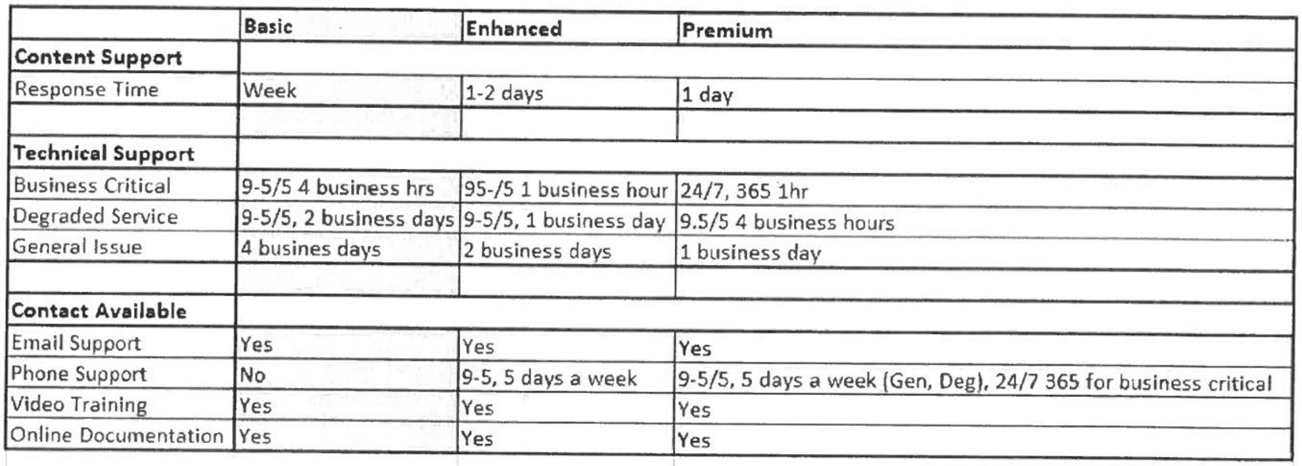
AppArmor will provide ongoing support to end-users of the App, including assistance with installing the App and using particular features of the App. End-users will be able to access this support via email.

2 Operating System and Device Updates

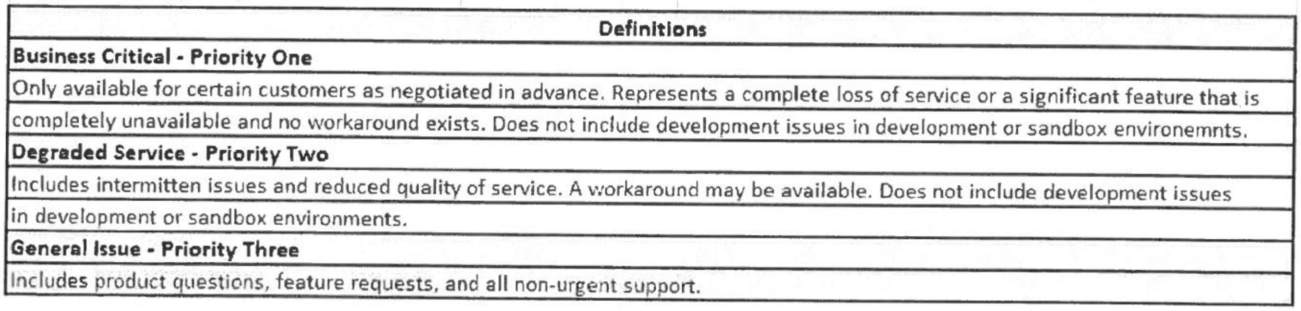
When new mobile devices and operating systems are released to the public, AppArmor will use reasonable efforts to update the App to ensure that the functionality specified in Schedule "A" is maintained, and resubmit the App to the applicable Distribution Platform(s) as necessary.

3 Bug Resolution

AppArmor will ensure that bugs are resolved within a reasonable time, and that the App is within a reasonable time resubmitted to the appropriate Distribution Platform(s) as necessary. Support SLAs are defined below. Customer qualifies for "Premium" Support. Uptime SLA guarantee of 99.9%.



	Basic	**Enhanced**	**Premium**
Content Support			
Response Time	Week	1-2 days	1 day
Technical Support			
Business Critical	9-5/5 4 business hrs	95-/5 1 business hour	24/7, 365 1hr
Degraded Service	9-5/5, 2 business days	9-5/5, 1 business day	9.5/5 4 business hours
General Issue	4 busines days	2 business days	1 business day
Contact Available			
Email Support	Yes	Yes	Yes
Phone Support	No	9-5, 5 days a week	9-5/5, 5 days a week (Gen, Deg), 24/7 365 for business critical
Video Training	Yes	Yes	Yes
Online Documentation	Yes	Yes	Yes



Definitions
Business Critical - Priority One
Only available for certain customers as negotiated in advance. Represents a complete loss of service or a significant feature that is
completely unavailable and no workaround exists. Does not include development issues in development or sandbox environemnts.
Degraded Service - Priority Two
Includes intermitten issues and reduced quality of service. A workaround may be available. Does not include development issues
in development or sandbox environments.
General Issue - Priority Three
Includes product questions, feature requests, and all non-urgent support.

4 Access to Online Dashboards

AppArmor will provide the Customer with password-protected access to an (or multiple) online dashboard (the "Online Dashboard"), which includes a content management system, location services features and the mass notification capability of the App. AppArmor will provide unlimited accounts for the Online Dashboard(s).

5 Resubmission to Distribution Platform

As described above, the Support Services include resubmission to Distribution Platforms in the case of: bug resolutions; and updates to the App in the case of new operating systems or devices. The Support Services further permit the Customer to request, at its discretion, up to one (1) resubmission per year to allow the Customer to gain access to any new features of the App.

6 Push Notifications

AppArmor will assist the Customer in deploying and monitoring the App's mass notification system. The Customer will be permitted to send an unlimited number of push notifications through this mass notification system.