AGREEMENT

This Agreement ("Agreement") is between the **Suffolk County Community College ("College")**, having its principal office at 533 College Road, Selden, New York 11784-2899, a community college established pursuant to New York State Education Law, under the sponsorship of the **County of Suffolk ("County")**, a municipal corporation of the State of New York; and

Intrado Interactive Services Corporation ("Contractor"), having a principal place of business at 1027 South Main Street, Suite 503, Joplin, Missouri 64801.

The parties hereto desire Contractor to provide a mobile communications system to enhance the College's ability to provide essential information to students through modern technological methods **("Services")**.

Term of Agreement: **March 1, 2020 to February 28, 2025**, with one (1) five-year (5-yr.) option to renew at the sole and absolute discretion of the College.

Total Cost of Agreement: Shall be as set forth in **Exhibit E**, attached hereto.

Terms and Conditions: Shall be as set forth in **Exhibits A through G**, attached hereto and made a part of this Agreement.

In Witness Whereof, the parties hereto have executed this Agreement as of the latest date written below.

Intrado Interactive Services Corporation
FID: 63-1078197
Tel.: (888) 527-5225 ext. 201

By: _____
Nate Brogan
President, Notification Services

Date: 3.10.2020

Suffolk County Community College

By: _____
Louis J. Petrizzo
Interim President

Date: 03/16/2020

Approved as to Legality:
Suffolk County Community College

By: _____
Alicia S. O'Connor
College Deputy General Counsel

Date: 3/11/2020

Approved:

By: _____
Mark D. Harris, DBA
Vice President for Business
& Financial Affairs

Date: MAR 1 1 2020

LIST OF EXHIBITS

Page

EXHIBIT A

General Terms and Conditions

Whereas, the College issued a Request for Proposals (RFP) on October 24, 2019*;* and

Whereas, the Contractor submitted a proposal in response to such RFP on December 11, 2019; and

Whereas, the College has selected the Contractor to provide the services as set forth herein; and

Now Therefore, in consideration of the mutual promises and covenants hereafter set forth, the parties hereto agree as follows:

1. Contractor Responsibilities

a. Services

The Contractor shall provide Services as described in Exhibit D, entitled "Description of Services."

b. Qualifications and Licenses

To the extent applicable, the Contractor specifically represents and warrants that it has and shall possess, and that, to the extent applicable, its employees, agents and subcontractors have and shall possess, the required education, knowledge, experience and character necessary to qualify them individually for the particular duties they perform and that the Contractor has and shall have, and, to the extent applicable, its employees, agents and subcontractors have and shall have, all required authorizations, certificates, certifications, registrations, licenses, permits or other approvals required by the State, County or other authorities for the Services provided.

2. Term and Termination

a. Term

This Agreement shall cover the period set forth on page one of this Agreement, unless sooner terminated as provided below. Upon receipt of a Termination Notice, as that term is defined below, pursuant to the following paragraphs, the Contractor shall promptly discontinue all Services affected, unless otherwise directed by the Termination Notice.

b. Termination

This Agreement may only be terminated in writing by either Party as follows (each a "Termination For Cause"):

i. By either party upon the failure by the other party to perform any material obligation hereunder that is not cured within thirty (30) days after receipt of written notice and demand for cure from the affected party.

ii. By either party upon the material violation by the other party of any applicable local, state or federal law, statute, rule or regulation, or College policy, in relation to its performance of this Agreement.

iii. By Contractor, upon thirty (30) days written notice if undisputed payments are in arrears. In addition, Contractor may suspend the Services any time undisputed payments are thirty (30) days in arrears.

iv. By College, in its sole discretion, upon a failure of the Contractor to maintain the amount and types of insurance required by this Agreement.

v. By College if Contractor becomes bankrupt or insolvent or falsifies its records or reports.

c. Effect of Termination.

In the event of any termination hereunder, College shall compensate Contractor for all Services rendered through the date of termination, as indicated in the Termination Notice.

i. Upon receiving a Termination Notice, Contractor shall promptly discontinue all services affected unless otherwise directed by the Termination Notice, and immediately return to College any and all College-owned materials, documents and data.

ii. The College shall be released from any and all responsibilities and obligations arising from the services provided in accordance with this Agreement, effective as of the date of termination, but the College shall be responsible for payment of all claims for services provided and costs incurred by Contractor prior to termination of this Agreement, that are pursuant to, and after Contractor's compliance with, the terms and conditions of this Agreement.

d. Termination for Emergencies

An emergency or other condition involving possible loss of life, threat to health and safety, destruction of property or other condition deemed to be dangerous, in the sole discretion of the College, may result in immediate termination of this Agreement, in whole or in part.

d. Intentionally Omitted

3. Indemnification.

a. General

Contractor agrees that it shall protect, indemnify and hold harmless the College and/or County and their officers, officials, employees, contractors, agents and other persons from and against all third party liabilities, fines, penalties, actions, damages, claims, demands, judgments, losses, costs, expenses, suits or actions and reasonable attorneys' fees, arising out of the negligent acts or omissions of Contractor in connection with the services described or referred to in this Agreement. Contractor shall defend the College and /or County and their officers, officials, employees, contractors, agents and other persons in any suit, including appeals, or at the College and /or County’s option, pay reasonable attorney’s fees for defense of any such suit arising out of the negligent acts or omissions of Contractor, its officers, officials, employees, subcontractors or agents, if any, in connection with the services described or referred to in this Agreement.

The College and/or County, to the extent permitted by law, agrees to indemnify and hold Contractor harmless from and against all liabilities, fines, penalties, actions, damages, claims, demands, judgments, losses, costs, expenses, suits or actions and reasonable attorneys' fees, arising out of the negligent acts or omissions of the College in connection with the services described or referred to in this Agreement. College shall defend Contractor and its officers, officials, employees and consultants, in any suit, including appeals arising out of negligent acts or omissions of the College, or at Contractor's option, pay reasonable attorney's fees for defense of any such suit arising out of the negligent acts or omissions of the College, its officers, officials, employees, subcontractors or agents, if any, in connection with the services described or referred to in this Agreement.

b. Contractor Intellectual Property Indemnity.

Contractor will have the obligation and right at the entire expense of Contractor to defend any claim, suit or proceeding brought against College its Affiliates or their officers, directors, employees or agents so far as it is based on a third party claim that the Services supplied by Contractor infringe a United States copyright or a United States patent issued as of the effective date of the Agreement, provided that Contractor will have no indemnity obligation or other liability hereunder arising from: (1) College's willful, reckless, wanton, wrongful, or otherwise negligent acts; (2) breach of the Agreement or alteration of the Services as provided by Contractor; (3) the College Systems and, or information, design, specifications, directions, instruction, software, data, or material not furnished by Contractor; (4) any materials, products or services not provided by Contractor; or any (5) third party products or services.

Notwithstanding the foregoing, in order to be indemnified to the extent stated, the College must operate the Licensed Materials within the instructions and technical limits provided or approved by the Contractor. If such a claim is or is likely to be made, Contractor will, at its own expense and sole discretion, exercise one or the following remedies: (1) obtain for College the right to continue to use the Services consistent with this Agreement; (2) modify the Services so they are non-infringing and in compliance with this Agreement; (3) terminate the applicable Services without liability for such termination other than the ongoing indemnity obligation hereunder. The foregoing states the entire obligation of Contractor and its suppliers, and the exclusive remedy of College, with respect to infringement of proprietary rights.

c. Indemnification Procedure.

The party claiming indemnification shall: (a) provide prompt written notice to the indemnifying party of any claim in respect of which the indemnity may apply; (b) relinquish control of the defense of the claim to the indemnifying party; and (c) provide the indemnifying party with all assistance reasonably requested in defense of the claim. The indemnifying party shall be entitled to settle any claim without the written consent of the indemnified party so long as such settlement only involves the payment of money by the indemnifying party and in no way affects any rights of the indemnified party. The indemnities set forth herein shall not apply to the willfulness on the part of the indemnified party or negligence of the indemnified party.

d. Federal Copyright Act

The College and the Contractor hereby represent and warrant that neither party will infringe upon any copyrighted work or material in accordance with the Federal Copyright Act during the performance of this Contract.

4. Insurance

a. Contractor agrees to procure, pay the entire premium for and maintain throughout the term of this Agreement, insurance in amounts and types specified by the College and as may be mandated and increased from time to time. Contractor agrees to require that all of its subcontractors, in connection with work performed for Contractor related to this Agreement, procure, pay the entire premium for and maintain throughout the term of this Agreement insurance in amounts and types equal to that specified by the College for Contractor. Unless otherwise specified by the College and agreed to by Contractor, in writing, such insurance shall be as follows:

i. **Commercial General Liability** insurance, including contractual liability coverage, in an amount not less than Two Million Dollars ($2,000,000.00) per occurrence for bodily injury and Two Million Dollars ($2,000,000.00) per occurrence for property damage.

ii. **Automobile Liability** insurance (if any vehicles are used by Contractor in the performance of this Agreement) in an amount not less than Five Hundred Thousand Dollars ($500,000.00) per person, per accident, for bodily injury and not less than One Hundred Thousand Dollars ($100,000.00) for property damage per occurrence.

iii. **Worker's Compensation** and **Employer's Liability** insurance in compliance with all applicable New York State laws and regulations and **Disability Benefits** insurance, if required by law. Contractor shall furnish to the College, prior to its execution of this Agreement, the documentation required by the State of New York Workers' Compensation Board of coverage or exemption from coverage pursuant to §§57 and 220 of the Workers' Compensation Law. In accordance with General Municipal Law §108, this Agreement shall be void and of no effect unless Contractor shall provide and maintain coverage during the term of this Agreement for the benefit of such employees as are required to be covered by the provisions of the Workers' Compensation Law.

b. All policies providing such coverage shall be issued by insurance companies with an A.M. Best rating of A- or better.

c. Contractor shall furnish to the College Declaration Pages for each such policy of insurance and upon request, a true and certified original copy of each such policy, evidencing compliance with the aforesaid insurance requirements. In the case of commercial general liability insurance, the College and the County of Suffolk shall be named as additional insureds and Contractor shall furnish a Declaration Page and endorsement page evidencing the College and the County's status as additional insureds on the policy.

d. Any such Declaration Page, certificate of insurance, policy, endorsement page or other evidence of insurance supplied to the College shall provide for the College and the County of Suffolk to be notified in writing thirty (30) days prior to any cancellation, nonrenewal or material change in the policies. Such Declaration Page, certificate of insurance, policy, endorsement page, other evidence of insurance and any notice of nonrenewal or material change shall be mailed to the College and the County at the addresses set forth in this Agreement in the exhibit entitled "Notices and Contact Persons" or at such other address of which the College and/or the County shall have given Contractor notice in writing.

e. In the event Contractor shall fail to provide the Declaration Page, certificate of insurance, policy, endorsement page or other evidence of insurance, or fails to maintain any insurance required by

this Agreement, the College and/or the County may, but shall not be required to, obtain such policies and deduct the cost thereof from payments due Contractor under this Agreement or any other agreement between the College and/or the County and Contractor.

5. Independent Contractor

It is expressly agreed that the Contractor's status hereunder is that of an independent contractor. Neither the Contractor, nor any person hired by the Contractor shall be considered employees of the College and/or the County for any purpose.

6. Severability

It is expressly agreed that if any term or provision of this Agreement, or the application thereof to any person or circumstance, shall be held invalid or unenforceable to any extent, the remainder of this Agreement, or the application of such term or provision to persons or circumstances other than those as to which it is held invalid or unenforceable, shall not be affected thereby, and every other term and provision of this Agreement shall be valid and shall be enforced to the fullest extent permitted by law.

7. Merger; No Oral Changes

It is expressly agreed that this Agreement represents the entire agreement of the parties and that all previous understandings are merged in this Agreement. No modification of this Agreement shall be valid unless written in the form of an Amendment and executed by both parties.

8. Set-Off Rights

The College and/or the County shall have all of its common law, equitable, and statutory rights of set-off. These rights shall include, but not be limited to, the College and/or the County's option to withhold, for the purposes of set-off, any moneys due to the Contractor under this contract up to any amounts due and owing to the College and/or County with regard to this contract and/or any other contract with the College or any County department or agency, including any contract for a term commencing prior to the term of this contract, plus any amounts due and owing to the College and/or the County for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto. The College and/or the County shall exercise its set-off rights in accordance with normal College and County practices including, in cases of set-off pursuant to an audit, the finalization of such audit by the College and/or the County, their representatives, or the County Comptroller, and only after legal consultation with the College General Counsel and County Attorney.

9. Non-Discrimination in Services

During the performance of this Agreement:

a. The Contractor shall not, on the grounds of race, creed, color, national origin, sex, age, disability, sexual orientation, military status or marital status:

i. deny any individual any services or other benefits provided pursuant to this Agreement; or

ii. provide any services or other benefits to an individual that are different, or are provided in a different manner, from those provided to others pursuant to this Agreement; or

iii. subject an individual to segregation or separate treatment in any matter related to the individual's receipt of any service(s) or other benefits provided pursuant to this Agreement; or

iv. restrict an individual in any way in the enjoyment of any advantage or privilege enjoyed by others receiving any services or other benefits provided pursuant to this Agreement; or

v. treat an individual differently from others in determining whether or not the individual satisfies any eligibility or other requirements or condition which individuals must meet in order to receive any aid, care, service(s) or other benefits provided pursuant to this Agreement.

b. The Contractor shall not utilize criteria or methods of administration which have the effect of subjecting individuals to discrimination because of their race, creed, color, national origin, sex, age, disability, sexual orientation, military status or marital status, or have the effect of defeating or substantially impairing accomplishment of the objectives of this Agreement in respect to individuals of a particular race, creed, color, national origin, sex, age, disability, sexual orientation, military status or marital status, in determining:

i. the types of service(s) or other benefits to be provided, or

ii. the class of individuals to whom, or the situations in which, such service(s) or other benefits will be provided; or

iii. the class of individuals to be afforded an opportunity to receive services.

10. College's Non-Discrimination Notice

Suffolk County Community College does not discriminate on the basis of race, color, religion, creed, sex, age, marital status, gender identity or expression, sexual orientation, familial status, pregnancy, predisposing genetic characteristics, equal pay compensation-sex, national origin, military or veteran status, domestic violence victim status, criminal conviction or disability in its admissions, programs and activities, or employment. This applies to all employees, students, applicants or other members of the College community (including, but not limited to, vendors and visitors). Grievance procedures are available to interested persons by contacting either of the Civil Rights Compliance Officers/Coordinators listed below and are located at www.sunysuffolk.edu/nondiscrimination. Retaliation against a person who files a complaint, serves as a witness, or assists or participates in the investigation of a complaint in any manner is strictly prohibited.

The following persons have been designated to handle inquiries regarding the College's non-discrimination polices:

Civil Rights Compliance Officers

Christina Vargas
Chief Diversity Officer/Title IX Coordinator
Ammerman Campus, NFL Bldg., Suite 230
533 College Road, Selden, New York 11784
vargasc@sunysuffolk.edu
(631) 451-4950

or

Dionne Walker-Belgrave
Affirmative Action Officer/Deputy Title IX Coordinator
Ammerman Campus, NFL Bldg., Suite 230
533 College Road, Selden, New York 11784
walkerd@sunysuffolk.edu
(631) 451-4051

11. Nonsectarian Declaration

The Contractor agrees that all services performed under this Agreement are secular in nature, that no funds received pursuant to this Agreement will be used for sectarian purposes or to further the advancement of any religion, and that no services performed under this program will discriminate on the basis of religious belief.

12. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws. Venues shall be designated in Suffolk County, New York or the United States District Court for the Eastern District of New York.

13. No Implied Waiver

No waiver shall be inferred from any failure or forbearance of the College and/or the County to enforce any provision of this Agreement in any particular instance or instances, but the same shall otherwise remain in full force and effect notwithstanding any such failure or forbearance.

14. Conflicts of Interest

a. The Contractor agrees that it will not during the term of this Agreement engage in any activity that is contrary to and/or in conflict with the goals and purposes of the College and/or the County.

b. The Contractor is charged with the duty to disclose to the College and/or the County the existence of any such adverse interests, whether existing or potential. This duty shall continue so long as the Contractor is retained on behalf of the College. The determination as to whether or when a conflict exists or may potentially exist shall ultimately be made by the College General Counsel and the County Attorney after full disclosure is obtained.

15. Cooperation on Claims

Each of the parties hereto agrees to render diligently to the other party, without additional compensation, any and all cooperation, that may be required to defend the other party, its employees and designated representatives against any claim, demand or action that may be brought against the other party, its employees or designated representatives in connection with this Agreement.

16. Confidentiality

Any records, reports or other documents of the College and/or the County or any of its agencies used by Contractor pursuant to this Agreement or any documents created as a part of this Agreement shall

remain the property of the College and/or the County and shall be kept confidential in accordance with applicable laws, rules and regulations.

17. Assignment and Subcontracting

a. The Contractor shall not assign, transfer, convey, sublet, or otherwise dispose of this Agreement, or any of its right, title or interest therein, or its power to execute the Agreement, or assign all or any portion of the monies that may be due or become due hereunder, to any other person or corporation, without the prior consent in writing of the College, and any attempt to do any of the foregoing without such consent shall be of no effect. Notwithstanding the foregoing, Contractor may freely assign this Agreement to an Affiliate or to an acquirer of all or part of Contractor's business or assets, whether by merger or acquisition.

b. The Contractor shall not enter into subcontracts for any of the work contemplated under this Agreement without obtaining prior written approval of the College. Such subcontracts shall be subject to all of the provisions of this Agreement and to such other conditions and provisions as the College and/or the County may deem necessary, provided, however, that notwithstanding the foregoing, unless otherwise provided in this Agreement, such prior written approval shall not be required for the purchase of articles, supplies, equipment and services which are incidental to, but necessary for, the performance of the work required under this Agreement. No approval by the College of any subcontract shall provide for the incurrence of any obligation by the College and/or the County in addition to the total agreed upon price. The Contractor shall be responsible for the performance of any subcontractor for the delivery of service.

18. No Intended Third Party Beneficiaries

This Agreement is entered into solely for the benefit of College and Contractor. No third party shall be deemed a beneficiary of this Agreement, and no third party shall have the right to make any claim or assert any right under this Agreement.

19. Certification as to Relationships

The parties to this Agreement hereby certify that, other than the funds provided in this Agreement and other valid Agreements with the College and/or the County, there is no known relationship within the third degree of consanguinity, life partner, or business, commercial, economic, or financial relationship between the parties, the signatories to this Agreement, and any partners, members, directors, or shareholders of five percent (5%) (or more) of any party to this Agreement.

20. Publications and Publicity

a. The Contractor shall not issue or publish any book, article, report or other publication related to the Services provided pursuant to this Agreement without first obtaining written prior approval from the College. Any such printed matter or other publication shall contain the following statement in clear and legible print:

"This publication is fully or partially funded by Suffolk County Community College and the County of Suffolk."

b. The College shall have the right of prior approval of press releases and any other information provided to the media, in any form, concerning the Services provided pursuant to this Agreement.

21. Copyrights and Patents

a. Copyrights

If the work of the Contractor under this Agreement should result in the production of original books, manuals, films or other materials for which a copyright may be granted, the Contractor may secure copyright protection. However, the College and/or the County reserves, and the Contractor hereby gives to the College and/or the County, and to any other municipality or government agency or body designated by the College and/or the County, a royalty-free, nonexclusive license to produce, reproduce, publish, translate or otherwise use any such materials.

b. Patents

If the Contractor under this Agreement makes any discovery or invention in the course of or as a result of work performed under this Agreement, the Contractor may apply for and secure for itself patent protection. However, the College and/or the County reserves, and the Contractor hereby gives to the College and/or the County, and to any other municipality or government agency or body designated by the College and /or the County, a royalty-free, nonexclusive license to produce or otherwise use any item so discovered or patented.

22. Limited Warranty and Limitation of Liability

a. EXCEPT AS EXPRESSLY PROVIDED HEREIN, PROVIDER MAKES NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES, AND PROVIDER EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. PROVIDER EXPRESSLY DENIES ANY REPRESENTATION OR WARRANTY ABOUT THE ACCURACY OR CONDITION OF DATA OR THAT THE SERVICES OR RELATED SYSTEMS WILL OPERATE UNINTERRUPTED OR ERROR-FREE.

b. NO CAUSE OR ACTION WHICH ACCRUED MORE THAN TWO (2) YEARS PRIOR TO THE FILING OF A SUIT ALLEGING SUCH CAUSE OF ACTION MAY BE ASSERTED UNDER THIS AGREEMENT BY EITHER PARTY.

c. EXCEPT FOR THE PARTIES' PAYMENT AND INDEMNIFICATION OBLIGATIONS, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY INDIRECT, EXEMPLARY, SPECIAL, PUNITIVE, CONSEQUENTIAL, OR INCIDENTAL DAMAGES OR LOSS OF GOODWILL, DATA OR PROFITS, OR COST OF COVER. THE TOTAL LIABILITY OF PROVIDER FOR ANY REASON, SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID TO PROVIDER BY COLLEGE UNDER THE CONTRACT APPLICABLE TO THE EVENT GIVING RISE TO SUCH ACTION DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY. THE LIMITS ON LIABILITY IN THIS SECTION SHALL APPLY IN ALL CASES INCLUDING IF THE APPLICABLE CLAIM ARISES OUT OF BREACH OF EXPRESS OR IMPLIED WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR STRICT PRODUCT LIABILITY, AND EVEN IF THE PARTY HAS BEEN ADVISED THAT SUCH DAMAGES ARE POSSIBLE OR FORESEEABLE.

23. Responsibility for Content, Transmitting Messages and Accounts

College represents and warrants that:

a. It is solely responsible for the content and it has the legal right to use all content and send all messages to the recipients (including obtaining any required consents from the recipients) and the content, timing and purpose of all messages, and College's campaigns and programs are in compliance with all applicable laws, rules and regulations;

b. College is the transmitter of all content and messages and contractor is merely acting at College's direction as a technology conduit for the transmission of the content and the messages;

c. Provider's use of the content shall not violate the rights of any third party or any law, rule or regulation;

d. College has prior express consent to contact each wireless phone number delivered by College to Contractor in connection with the provision of any Services delivering a prerecorded or text message ("Notification Services"), or the Notification Services are made for an emergency purpose not requiring prior express consent;

e. The intended contact recipient is, to the College's knowledge, the current subscriber to, or the non-subscriber customary user of, the wireless phone number;

f. Upon request by Provider, College shall promptly provide, in writing, proof of prior express consent and College's processes for consent management.

g. College has (a) incorporated an interactive opt-out mechanism as part of any program relating to any Notification Services or (b) the contacts that are the subject of such Notification Services are not initiated to induce the purchase of goods or services or to solicit a charitable contribution; and College will not transmit or allow to be transmitted any content or messages that: (a) it does not have a right to make available under any law or under contractual or fiduciary relationship; (b) are false, inaccurate, misleading, unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable; harmful to minors in any way; (c) infringe any patent, trademark, trade secret, copyright, or other proprietary rights or rights of publicity or privacy of any party; (d) utilize any unsolicited or unauthorized advertising, promotional materials, "junk mail", "spam", or any other forms of solicitation; or (e) interfere with or disrupts the Services or servers or network operator networks.

h. Upon request, College shall provide reasonable proof of compliance with the provisions set forth in this section and where Contractor reasonably believes that College may not have complied with such provisions or with all laws, rules and regulations, Contractor shall notify College of the same, stating the basis for such belief, in writing. If the College fails to cure any such non-compliance within thirty (30) days after receipt of written notice and demand for cure, Contractor may, at its option (i) scrub all numbers against any appropriate data base deemed necessary to remove all wireless phone numbers, (ii) insert an interactive opt-out mechanism and pass the resulting data to College or (iii) not provide any Services until College provides reasonable proof of compliance.

i. College shall indemnify, defend and hold Contractor, its affiliates and their officers, directors, employees and agents harmless from and against any and all claims of loss, damages, liability, costs, and expenses (including reasonable attorneys' fees and expenses) arising out of or resulting from College's breach of any representation and warranty set forth in this section.

End of Text for Exhibit A

EXHIBIT B

Suffolk County Legislative Requirements

1. Contractor's/Vendor's Public Disclosure Statement

The Contractor represents and warrants that it has filed with the Comptroller of Suffolk County the verified public disclosure statement required by Suffolk County Administrative Code Article V, Section A5-7 and shall file an update of such statement with the said Comptroller on or before the 31st day of January in each year of this Agreement's duration. The Contractor acknowledges that such filing is a material, contractual and statutory duty and that the failure to file such statement shall constitute a material breach of this Agreement, for which the College shall be entitled, upon a determination that such breach has occurred, to damages, in addition to all other legal remedies, of fifteen percent (15%) of the amount of the Agreement.

Required Form: Suffolk County Form SCEX 22; entitled "Contractor's/Vendor's Public Disclosure Statement"

2. Living Wage Law

This Agreement is subject to the Living Wage Law of the County of Suffolk. The law requires that, unless specific exemptions apply all employers (as defined) under service contracts and recipients of County financial assistance, (as defined) shall provide payment of a minimum wage to employees as set forth in the Living Wage Law. Such rate shall be adjusted annually pursuant to the terms of the Suffolk County Living Wage Law of the County of Suffolk. Under the provisions of the Living Wage Law, the County shall have the authority, under appropriate circumstances, to terminate this Agreement and to seek other remedies as set forth therein, for violations of this Law.

The Contractor represents and warrants that it has read and shall comply with the requirements of Suffolk County Code Chapter 347, Suffolk County Local Law No. 12-2001, the Living Wage Law.

Required Forms: Suffolk County Living Wage Form LW-1; entitled "Suffolk County Department of Labor – Living Wage Unit Notice of Application for County Compensation (Contract)"

Suffolk County Living Wage Form LW-38; entitled "Suffolk County Department of Labor – Living Wage Unit Living Wage Certification/Declaration – Subject To Audit"

3. Use of County Resources to Interfere with Collective Bargaining Activities Local Law No. 26-2003

The Contractor represents and warrants that it has read and is familiar with the requirements of Chapter 466, Article 1 of the Suffolk County Local Laws, "Use of County Resources to Interfere with Collective Bargaining Activities." County Contractors (as defined) shall comply with all requirements of Local Law No. 26-2003 including the following prohibitions:

a. The Contractor shall not use County funds to assist, promote, or deter union organizing.

b. No County funds shall be used to reimburse the Contractor for any costs incurred to assist, promote, or deter union organizing.

c. The County of Suffolk shall not use County funds to assist, promote, or deter union organizing.

d. No employer shall use County property to hold a meeting with employees or supervisors if the purpose of such meeting is to assist, promote, or deter union organizing.

If Contractor services are performed on County property the Contractor must adopt a reasonable access agreement, a neutrality agreement, fair communication agreement, nonintimidation agreement and a majority authorization card agreement.

If Contractor services are for the provision of human services and such services are not to be performed on County property, the Contractor must adopt, at the least, a neutrality agreement.

Under the provisions of Local Law No. 26-2003, the County shall have the authority, under appropriate circumstances, to terminate this Agreement and to seek other remedies as set forth therein, for violations of this Law.

Required Form: Suffolk County Labor Law Form DOL-LO1; entitled "Suffolk County Department of Labor – Labor Mediation Unit Union Organizing Certification/Declaration – Subject to Audit"

4. Lawful Hiring of Employees Law

This Agreement is subject to the Lawful Hiring of Employees Law of the County of Suffolk (Local Law 52-2006). It provides that all covered employers, (as defined), and the owners thereof, as the case may be, that are recipients of compensation from the County through any grant, loan, subsidy, funding, appropriation, payment, tax incentive, contract, subcontract, license agreement, lease or other financial compensation agreement issued by the County or an awarding agency, where such compensation is one hundred percent (100%) funded by the County, shall submit a completed sworn affidavit (under penalty of perjury), certifying that they have complied, in good faith, with the requirements of Title 8 of the United States Code Section 1324a with respect to the hiring of covered employees (as defined) and with respect to the alien and nationality status of the owners thereof. The affidavit shall be executed by an authorized representative of the covered employer or owner, as the case may be; shall be part of any executed contract, subcontract, license agreement, lease or other financial compensation agreement with the County; and shall be made available to the public upon request.

All contractors and subcontractors (as defined) of covered employers, and the owners thereof, as the case may be, that are assigned to perform work in connection with a County contract, subcontract, license agreement, lease or other financial compensation agreement issued by the County or awarding agency, where such compensation is one hundred percent (100%) funded by the County, shall submit to the covered employer a completed sworn affidavit (under penalty of perjury), certifying that they have complied, in good faith, with the requirements of Title 8 of the United States Code Section 1324a with respect to the hiring of covered employees and with respect to the alien and nationality status of the owners thereof, as the case may be. The affidavit shall be executed by an authorized representative of the contractor, subcontractor, or owner, as the case may be; shall be part of any executed contract, subcontract, license agreement, lease or other financial compensation agreement between the covered employer and the County; and shall be made available to the public upon request.

An updated affidavit shall be submitted by each such employer, owner, contractor and subcontractor no later than January 1 of each year for the duration of any contract and upon the renewal or amendment of the contract, and whenever a new contractor or subcontractor is hired under the terms of the contract.

The Contractor acknowledges that such filings are a material, contractual and statutory duty and that the failure to file any such statement shall constitute a material breach of this agreement.

Under the provisions of the Lawful Hiring of Employees Law, the County shall have the authority to terminate this Agreement for violations of this Law and to seek other remedies available under the law.

This Agreement is subject to the Lawful Hiring of Employees Law of the County of Suffolk, Suffolk County Code Chapter 234, as more fully set forth in Exhibit B collectively referred to as the "Suffolk County Legislative Requirements." In accordance with this law, Contractor or employer, as the case may be, and any subcontractor or owner, as the case may be, agree to maintain the documentation mandated to be kept by this law on site at all times. Contractor or employer, as the case may be, and any subcontractor or owner, as the case may be, further agree that employee sign-in sheets and register/log books shall be kept on site at all times during working hours and all covered employees, as defined in the law, shall be required to sign such sign in sheets/register/log books to indicate their presence on the site during such working hours.

The Contractor represents and warrants that it has read, is in compliance with, and shall comply with the requirements of Suffolk County Code Chapter 234, Suffolk County Local Law No. 52-2006, the Lawful Hiring of Employees Law.

Required Forms: Suffolk County Lawful Hiring of Employees Law Form LHE-1; entitled “Suffolk County Department of Labor –”Notice Of Application To Certify Compliance With Federal Law (8 U.S.C. SECTION 1324a) With Respect To Lawful Hiring of Employees”

“Affidavit Of Compliance With The Requirements Of 8 U.S.C. Section 1324a With Respect To Lawful Hiring Of Employees” Form LHE-2.

5. Gratuities

The Contractor represents and warrants that it has not offered or given any gratuity to any official, employee or agent of Suffolk County or New York State or of any political party, with the purpose or intent of securing an agreement or securing favorable treatment with respect to the awarding or amending of an agreement or the making of any determinations with respect to the performance of an agreement, and that the signer of this Agreement has read and is familiar with the provisions of Local Law No. 32-1980 of Suffolk County (Chapter 386 of the Suffolk County Code).

6. Prohibition Against Contracting with Corporations that Reincorporate Overseas

The Contractor represents that it is in compliance with Suffolk County Administrative Code Article IV, §§A4-13 and A4-14, found in Suffolk County Local Law No. 20-2004, entitled “A Local Law To Amend Local Law No. 5-1993, To Prohibit The County of Suffolk From Contracting With Corporations That Reincorporate Overseas.” Such law provides that no contract for consulting services or goods and services shall be awarded by the County to a business previously incorporated within the U.S.A. that has reincorporated outside the U.S.A.

7. Child Sexual Abuse Reporting Policy

The Contractor agrees to comply with Chapter 577, Article IV, of the Suffolk County Code, entitled "Child Sexual Abuse Reporting Policy", as now in effect or amended hereafter or of any other Suffolk County Local Law that may become applicable during the term of this Agreement with regard to child sexual abuse reporting policy.

8. Non-Responsible Bidder

The Contractor represents and warrants that it has read and is familiar with the provisions of Suffolk County Code Chapter 143, Article II, §§143-5 through 143-9. Upon signing this Agreement the Contractor certifies that he, she, it, or they have not been convicted of a criminal offense within the last ten (10) years. The term "conviction" shall mean a finding of guilty after a trial or a plea of guilty to an offense covered under the provision of Section 143-5 of the Suffolk County Code under "Nonresponsible Bidder."

9. Use of Funds in Prosecution of Civil Actions Prohibited

Pursuant to the Suffolk County Code Section §590-3, the Contractor represents that it shall not use any of the moneys received under this Agreement, either directly or indirectly, in connection with the prosecution of any civil action against the County of Suffolk or any of its programs, funded by the County, in part or in whole, in any jurisdiction or any judicial or administrative forum.

10. Suffolk County Local Laws

Suffolk County Local Laws, Rules and Regulations can be found on the Suffolk County website at http://suffolkcountyny.gov/.

End of Text for Exhibit B

EXHIBIT C

Notices and Contact Persons

1. Notices Relating to Reports, Insurance or Other Submissions

Any communication, notice, report, insurance, or other submission necessary or required to be made by the parties regarding this Agreement shall be in writing and shall be given to the College or Contractor or their designated representative at the following addresses or at such other address that may be specified in writing by the parties and must be delivered as follows:

For the College:

Vice President for Business and Financial Affairs
Suffolk County Community College
533 College Road, NFL-232
Selden, NY 11784-2899

and

For Contractor:

At the address set forth on page one of this Agreement, attention of the person who executed this Agreement or such other designee as the parties may agree in writing.

Notices for all parties (except those related to termination or litigation) should be delivered by first class and certified mail, return receipt requested, in a postpaid envelope or by courier service, or by fax or by email.

2. Notices Relating to Payments

Any communication, notice or claim relating to payment by the parties regarding this Agreement shall be in writing and shall be given to the College or Contractor or their designated representative at the following addresses or at such other address that may be specified in writing by the parties and must be delivered as follows:

For the College:

Vice President for Business and Financial Affairs
Suffolk County Community College
533 College Road, NFL-232
Selden, NY 11784-2899

and

For Contractor:

At the address set forth on page one of this Agreement, attention of the person who executed this Agreement or such other designee as the parties may agree in writing.

Notices for all parties (except those related to termination or litigation) should be delivered by first class and certified mail, return receipt requested, in a postpaid envelope or by courier service, or by fax or by email.

3. Notices Relating to Termination and/or Litigation

In the event the Contractor receives a notice or claim or becomes a party (plaintiff, petitioner, defendant, respondent, third party complainant, third party defendant) to a lawsuit or any legal proceeding related to this Agreement, the Contractor shall immediately deliver to the Office of Legal Affairs and the County Attorney, at the addresses set forth below, copies of all papers filed by or against the Contractor.

Any communication or notice regarding termination shall be in writing and shall be given to the College or the Contractor or their designated representative at the following addresses or at such other addresses that may be specified in writing by the parties and must be delivered as follows:

For the College and County:

Office of Legal Affairs
Suffolk County Community College
533 College Road, NFL Bldg., Suite 230
Selden, NY 11784-2899

and

Suffolk County Attorney
Suffolk County Department of Law
H. Lee Dennison Building
100 Veterans Memorial Highway
Hauppauge, NY 11788-5402

And

For Contractor:

At the address set forth on page one of this Agreement, attention of the person who executed this Agreement or such other designee as the parties may agree in writing.

Notices related to termination or litigation should be delivered by first class and certified mail, return receipt requested, in a postpaid envelope or by nationally recognized courier service or personally and by first class mail.

Notices shall be deemed to have been duly delivered: (i) if mailed, upon the seventh business day after the mailing thereof; or (ii) if by nationally recognized overnight courier service, upon the first business day subsequent to the transmittal thereof; or (iii) if personally, pursuant to New York Civil Practice Law and Rules Section 311; or (iv) if by fax or email, upon the transmittal thereof. "Business Day" shall be defined as any day except a Saturday, a Sunday, or any day in which commercial banks are required or authorized to close in Suffolk County, New York.

Each party shall give prompt written notice to the other party of the appointment of successor(s) to the designated contact person(s) or his or her designated successor(s).

End of Text for Exhibit C

EXHIBIT D
Description of Services

Section III
Scope of Work

I. GENERAL INFORMATION

The Consultant shall provide services in connection with the implementation of a secure, web-based mobile communication system at the College, which at a minimum, meets the requirements and components identified below. All databases, reports and other materials developed and prepared by the Consultant in connection with this agreement are the sole property of the College.

II. SYSTEM REQUIREMENTS

- Ability for multiple entities to create and send text and email messages to individuals and groups of subscribers
- Ability to provide more than 50 message categories so that users can select the content they prefer to receive via text message, email or both
- Ability to send text and email messages immediately, as well as through advance and recurring scheduling functions
- Customizable messaging capabilities that include inserting graphics, images, URLs, e-blasts, and templates
- Ability to import text or an established list of subscribers and provide a seamless transition from an existing system
- Automated sign-up (opt in or opt out) application accessible to computer, smartphone and tablet users
- Customizable sign-up (opt in or opt out) interface for customer-facing aspects of the application
- Ability to communicate with targeted audience via text, email and phone message automatically
- Administrative access to manage message creation, subscriber database, message log, advance/recurring delivery and individual access accounts
- Robust subscription and usage reporting capabilities
- Compliance with the CAN-spam Act of 2003 and FCC regulations
- API that extracts data from Banner
- Ability to upload users and criteria into system
- Ability to post to social media applications and RSS feeds
- Ability to connect to LCD screens
- Emergency and non-emergency message hosted off site
- System shall be able to connect to College's active directory for authentication and LDAP
- CAS certified

III. IMPLEMENTATION SCHEDULE

The system shall be implemented and ready for use no later than February 24, 2020.

IV. TRAINING

The Consultant shall provide training to College staff prior to the system being put into service, as well as ongoing training for new employees on an as-needed basis throughout the term of the Contract. Consultant shall provide all necessary audiovisual and printed materials, as well as instructors for this purpose. All capabilities and controls shall be demonstrated and all service requirements shall be reviewed during the training sessions.

V. CUSTOMER SERVICE

The Consultant shall be responsible for providing customer service to subscribers on an as-needed basis throughout the term of the Contract.

End of text for Section III

IV. TECHNICAL PROPOSAL

RFP No. R20-002

IV. TECHNICAL PROPOSAL

a) Understanding of Project Requirements, Management Techniques and Approaches

UNDERSTANDING OF THE SYSTEM REQUIREMENTS

Convey your understanding of the requirements for the software or hosted system by describing how your solution meets the needs identified in Section III – Scope of Work.

STATEMENT OF UNDERSTANDING

We understand SCCC's goals of this project to include:

- A high-speed, vendor-hosted automated communication system;
- Message delivery via voice, email, text, social media, and mobile app;
- Ongoing training and technical support; and,
- A robust mobile app for sending and receiving messages.

The same SchoolMessenger solution trusted by Suffolk County Community College to send over 3.59 Million notifications over the past 12 months!

The system should support SCCC campuses and should be scalable as the College continues to grow. Additionally, the system should provide integration with the College's existing Ellucian Banner Student Information System and other databases and must provide maximum availability.

OUR SOLUTION

To meet the needs outlined by SCCC, we are proposing continued deployment of our fully hosted mass notification system: SchoolMessenger Communicate – the same solution SCCC has trusted since 2014 to meet your daily communication needs . SchoolMessenger features:

- Voice, SMS Text, E-mail, Push Notification, Desktop Alert, RSS, / Website delivery options;
- The deepest educational feature set in the market (including a recipient app); and,
- Maximum uptime, security, and reliability.

In fact, this solution meets the requirements outlined by SCCC and for added value, we also include:

- Our award-winning, 24/7/365 truly unlimited support;
- Full implementation support including a dedicated project manager; and,
- Customizable training options that are designed to fit your unique needs and schedule.

On the following pages, we've outlined the capabilities of our solution, industry experience and a commitment to excellence that will help ensure the continued success of this important and highly visible project.

SOLUTION DETAILS

SCHOOLMESSENGER COMMUNICATE

From emergency communication capabilities that are ready for any crisis to best-in-class tools for community and classroom engagement, SchoolMessenger Communicate is the unrivaled notification solution for higher education as well as K-12 schools and districts.

Simply put, SchoolMessenger Communicate delivers in the most critical situations, and that's why the product consistently outscores other systems in rigorous evaluations by

the most demanding institutions. What's more, SchoolMessenger Communicate is shown to positively impact academic achievement, increase community involvement, and save staff time.

For a notification system you can count on in critical situations, choose SchoolMessenger Communicate.

SchoolMessenger Communicate Offers the Following:

Unmatched Reliability and Performance

- ✓ **We've built the largest communications network in education,** offering unequaled capacity, infrastructure, and speed to help deliver your important messages efficiently and effectively;

- ✓ **We deliver millions of messages at once and more than a billion messages per year** – all with precise accuracy and high speed, even during peak times;

- ✓ **Patented technology ensures rapid message distribution** – Thanks to our sophisticated, proprietary algorithms, your important notifications don't have to "wait in line" behind notifications from other institutions; and,

- ✓ **Time-tested technology that has delivered in every possible circumstance** – We've successfully delivered time-sensitive notifications about every kind of event, including violence incidents, severe weather events, lockdowns, and unexpected campus closures.

Deepest Educational Feature Set

- ✓ **The most full-featured messaging product for higher education** – Send unlimited broadcasts using voice, text, email, social media, desktop pop-up, web, and push notifications from one simple screen;

- ✓ **Integration and automation with more than 130 data sources** – Powerful integration capabilities with popular education software, including SIS and HRIS data integration;

- ✓ **Instant translation to more than 100 languages** – Featuring robust text to speech, text to text, and quality assurance tools;

- ✓ **Free SchoolMessenger app and portal** – Connect the community with an app that brings together rich messaging technology with campus- and College-level notifications; available for free as a mobile Apple or Android app and as a web-based portal;

- ✓ **Industry-leading TCPA compliance tools** that make it easier for you to stay compliant with important federal regulations on phone and text message communications and avoid costly lawsuits;

- ✓ **Hands-free notifications for every situation**;

- ✓ **Powerful yet simple interface** – Staff of all skill levels report that Communicate is amazingly easy to learn and use;

- ✓ **Complex scenario handling** – Control how messages are delivered based on the notification type (e.g. early morning closure calling home phones versus afternoon dismissals calling mobile and work phones) – also set College-wide defaults and even configure individual rules to handle student-specific scenarios;

- ✓ **Easy cross-platform communication** – Send notifications from Communicate and automatically update your website and mobile app, saving you time and effort;

- ✓ **Powerful reporting and analytics** – Select from dozens of standard reports or build your own; save and schedule reports to automate processes such as "bad number" clean up; monitor activity in real time;

- ✓ **Social media integration** – Easily publish to multiple Facebook and Twitter accounts at once from directly within the familiar Communicate interface; post voice messages to Facebook effortlessly;

- ✓ **Robust email messaging tools** – Let us create beautiful HTML templates for your email newsletters or create and edit on your own with our template editor; powerful email analytics show you who opened and how much time they spent on your email;

- ✓ **Flexible management tools** – Streamline deployment and support; authenticate against LDAP-aware data sources; securely publish list definitions and messages between users;

- ✓ **Interactive notification features** – Capture voice responses, and send surveys through phone and web with an unlimited number of questions;

- ✓ **Access anywhere with our iPhone and Android broadcasting apps; and,**
- ✓ **Hundreds more features and functionalities**

SCHOOLMESSENGER APP

When it comes to community engagement, one of the biggest challenges educators face is avoiding message fatigue. That's because there are so many communications tools available, and often, different tools are being used by the same organization.

The new SchoolMessenger app was built to address this challenge. The SchoolMessenger app – ***available for free as a mobile app for Apple and Android devices and as a web-based application*** – brings together rich messaging technology with campus- and College-level notifications.

This provides users with a single app for all of their communications, and gives College leaders more visibility into, and control over, messaging. Learn more about how the SchoolMessenger app can improve engagement in your community.

Key Benefits of the SchoolMessenger App:
Powerful Tools to Keep Users Connected

- ✓ **One simple, scrollable, streamlined view** that allows users to view private messages, group texts, and notifications in one convenient place, just as they would on any other popular app or social media site (see screenshot above);
- ✓ **Users can engage in two-way conversations** with groups (i.e. classrooms, sports teams, PTO groups, etc.) and individuals (i.e., instructors);
- ✓ **Multimedia messaging options** that allow users to exchange files, images, and videos with instructors; and,

- ✓ **All the tools users need to stay connected** to their education – no need to sign up for multiple communications channels or switch between multiple communications apps to get the information they need!

UNMATCHED SERVICE

Support That Exceeds Expectations

Unlike other communications products, SchoolMessenger solutions come with ***truly unlimited, 24/7/365 support – at no extra charge***. There is no limit on the number of support cases you can submit and no cost for "premium" support. In addition, we never place restrictions on the number of people in your organization who can contact our support team. Any staff member that has been trained on the system can contact us anytime with questions on any type of issue.

What's more, we realize that switching communications providers can pose a challenge. That is why we make the process as painless as possible with ***free implementation support***. Whether you call our toll-free 800 number, submit a support ticket via email, start a live chat, or contact us via web form, you will discover the difference that world-class service can make.

Tested, Trusted, and Reliable Technology

SchoolMessenger products run on ***the world's largest communications network***. Many of the Canada and the United States most demanding educational organizations trust their important communications to SchoolMessenger products. SchoolMessenger products are also ***recognized by leading edtech organizations and industry publications***:

In addition, we were ***an early signatory of the Student Privacy Pledge***, which was created by The Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) to encourage school service providers to affirm that student information is kept private and secure. We adhere to the

Pledge's twelve stringent standards as part of a complete commitment to protecting student data.

Top Notch Training

We offer a range of ***customizable training options*** to get your users confident and ready to use our system to its fullest potential. Let our experienced trainers help ensure your users are trained effectively on the system. Additionally, the learning resources available through our Resource Central offer product news, tips and tricks, training modules, and more.

RESPONSE TO SECTION III – SCOPE OF WORK

II. System Requirements

Ability for multiple entities to create and send text and email messages to individuals and groups of subscribers

---

✓ Yes. SchoolMessenger supports an unlimited number of security profiles. Each profile can be granularly controlled to provide various levels of access to the system. The rights of each profile-type — whether it be System Administrator, College Administrator, Campus Administrator, or one of an unlimited number of profiles that the College wishes created – are highly configurable. Also, all list creation is set by the user's security profile (e.g. a campus administrator's lists may contain only contacts from within that campus administrator's school; while a college administrator's lists may contain any contacts in the college).

And, list creation is a powerful function in SchoolMessenger. Users simply select their audience from their available data set, and then their lists are dynamically and automatically updated based on the most current data. When changes occur in the student information system, the lists in SchoolMessenger automatically update to reflect the new changes. So, when a new student joins Gateway Community College, the "Gateway Community College Students" list is automatically updated. And the college maintains complete assurance that a user only has access to the self-updating lists they are supposed to have access to.

Ability to provide more than 50 message categories so that users can select the content they prefer to receive via text message, email or both

✓ Yes. Notification types can be associated with one or more delivery points (e.g. call phone #1 for a Tuition Call; call phone #1, #2 and #3 plus all email addresses for an Emergency; use email # 2 for Surveys, etc.). To accommodate special needs of the campus, this capability is fully configurable system-wide, configurable for individual student records.

Ability to send text and email messages immediately, as well as through advance and recurring scheduling functions

✓ Yes. SchoolMessenger supports the immediate sending of notifications or the scheduling of jobs by specific days/dates/times – even years in advance. Message times and job lengths can also be restricted on a user-by-user basis. Plus, jobs can easily be configured to run on a routine, scheduled basis.

Customizable messaging capabilities that include inserting graphics, images, URLs, e-blasts, and templates

✓ Yes. With SchoolMessenger you get the option to brand your outbound email messages with your organization's logo and colors. Now every time they receive a SchoolMessenger email, recipients will see the logo, look, and feel they've come to associate with your organization. And using the included portal functionality, recipients can easily sign up for just the topics they are interested in. See below for additional details.

And, SchoolMessenger supports multiple direct attachments and links (pointers to external files). The user simply browses for and uploads the files or uses a link to point to them externally.

Enhanced Email Stationary

The system offers a built-in module that provides SCCC with a full suite of email options that allows for a fine degree of branding and central office control. And, best of all, these

templates are designed to be responsive and adapt to the recipient's device's size. Details follow:

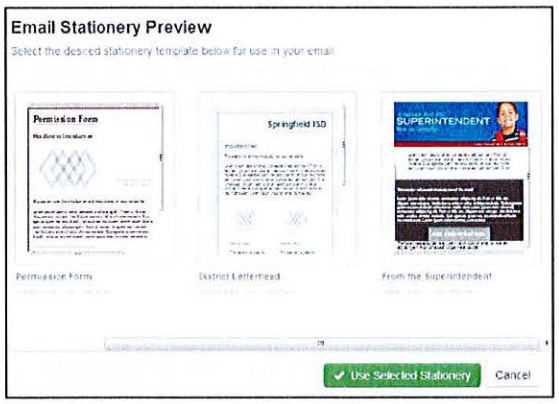
Email Features

The system allows novices and power users alike to create beautiful emails complete with graphics and rich layouts. Highlights include:

- HTML and plain text editing options;
- Unlimited number of attachments of up to 50 MB in size;
- Handy "Paste from Word" and "Remove Format" buttons to paste content without the extra, non-standard information often attached to content from other editors;
- Editable "from" and "reply-to" addresses; and
- Dynamic data fields that can be automatically inserted into any email message.

Email Templates

The system provides responsive email templates that enable SCCC to brand outbound email messages with your logo and colors. Now every time you send an email, your recipients will see the logo and 'look and feel' they have come to associate with your organization.



The layout templates allow administrators to customize email layout to meet each schools' needs, while the lockdown feature ensures each email from SCCC will have a standardized look.

Email Tracking

The system provides all users with web browser access to many reports. Each user's security profile governs his or her access to system reports. This means that a school-

level user has access to data at the department-level only, while a campus-level user has access to data at the campus-wide level.

The Email Log report displays the results of an email broadcast, including open rates, number of attempts, last delivery attempted, and delivery results, all at a recipient level.

Detailed Status Logs

Easily see and export detailed results for every email broadcast. In addition to seeing open rates for every single email, you get granular statistics about email delivery including various "bounce" statuses, which can help troubleshoot bad email addresses. Everything is logged so you have a full audit trail documenting your communication efforts.

Ability to import text or an established list of subscribers and provide a seamless transition from an existing system

✓ Not applicable. ***As the current provider of SCCC's notification services,*** upon renewal, service will continue uninterrupted. Moreover, since your staff and administrators are already fully trained and familiar with SchoolMessenger (which has been ***deployed within your College since 2014***), renewal will be a breeze. This existing familiarity means that there will be no need for training (beyond refresher training), and there will be no lengthy implementation processes.

Automated sign-up (opt in or opt out) application accessible to computer, smartphone and tablet users

✓ Yes. SchoolMessenger includes self-sign-up for recipients to perform self-service updating of contact information, opting in/out of different notification types, and reviewing of past messages through the Web. This portal is optional and not required.

Customizable sign-up (opt in or opt out) interface for customer-facing aspects of the application

---

✓ Yes. SchoolMessenger includes self-sign-up for recipients to perform self-service updating of contact information, opting in/out of different notification types, and reviewing of past messages through the Web. This portal is optional and not required.

Ability to communicate with targeted audience via text, email and phone message automatically

---

✓ Yes. SchoolMessenger rapidly delivers messages to unlimited landline phones, cellular phones (voice and text/SMS), smartphones, unlimited e-mail addresses, and social media sites like Facebook and Twitter. Plus, SchoolMessenger directly updates RSS feeds and college websites. ***Any combination of these delivery methods is supported in any broadcast.***

Administrative access to manage message creation, subscriber database, message log, advance/recurring delivery and individual access accounts

---

✓ Yes. SchoolMessenger supports an unlimited number of security profiles. Each profile can be granularly controlled to provide various levels of access to the system. The rights of each profile-type — whether it be System Administrator, College Administrator, Campus Administrator, or one of an unlimited number of profiles that the Colleges wish created – are highly configurable. Also, all list creation is set by the user's security profile (e.g. a campus administrator's lists may contain only contacts from within that campus administrator's school; while a college administrator's lists may contain any contacts in the college).

Robust subscription and usage reporting capabilities

✓ Yes. The system provides all users with web browser access to numerous reports. All report access is governed by each user's security profile. This means that a campus-level user has access to data at the campus-level only, while an administrator-level user has access to data at the College-wide level.

Users can analyze out-of-the-box reports provided by the system. Alternatively, use the system's rich ad hoc reporting features, which allows on the fly querying of most any data elements. The system also excels in producing notification-history reports. These reports can look at any combination of call statuses including busy, answering machine, disconnected number, no answer, answered by person, etc.

An unlimited number of reports can be created. Here are some common ones including the benefits to administrators:

- **Individual Contact History** – useful for showing all notification attempts to a single phone number or single contact ID. Even filter by notification type or call results (e.g. show only answered calls);
- **Full Log Reporting** – provides an easy web-based user interface for querying most any system element including all notification attempts and results by channel (voice call, SMS text, email), by user, by campus, or by any other criteria such as contact group association, language, message, etc.;
- **Current Activity** – a single dashboard report for authorized administrators to view / modify / cancel current system activity such as active or queued notifications;
- **Contact Information Changes** – provides a report and export showing all changes to contact information made by users over a configurable date range. This export can even be scheduled. Many clients optionally use this report to identify recent changes made to student contact information so they can automatically import (or manually key in) the updated fields into the source Student Information System (SIS);
- **Interaction Reports** – including survey reports (unlimited number of questions / responses), touchtone captures, and voice replies;
- **Usage Statistics by Campus and by User** – creates an account-wide comparative report for identifying those performing at, above, or below expectations for communication activity;

- **User Account Reports** – including user ID, name, contact information, last login information, activity, staff key (used in optional LDAP authentication), profile, data view restriction, job type restriction, section restrictions, other restrictions, organizational associations, and custom fields;
- **Call Distribution Reports** – including average system-wide daily and hourly volume and total system-wide volume;
- **Blocked Recipient Reports** – shows those who have been opted out by authorized Administrators from receiving notifications; and,
- **Data Import Reports** – indicates data last run and status of every automated import (e.g. from SIS and other data sources). Includes detailed log of import activity with line-by-line alarms for such things as malformed data, file smaller / larger than expected, etc.

Most every report can be customized to show or hide columns, filter or sort by any criteria, export to CSV or print to PDF / printer, and ***even be saved and scheduled.*** For example, it is easy to set a report of campus-specific disconnected numbers to automatically be emailed every Friday to the data processing clerks at each campus, or to have a College-wide benchmarking report emailed to administrative staff on the last day of every month.

Compliance with the CAN-spam Act of 2003 and FCC regulations

✓ Yes. SchoolMessenger complies with the CAN-SPAM act and FCC regulations.

API that extracts data from Banner

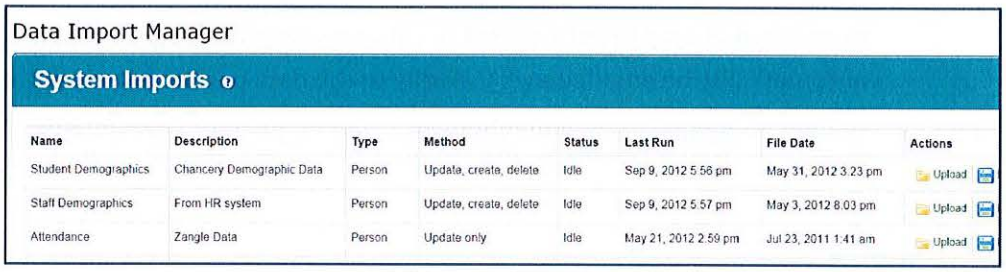
✓ Yes. ***As SCCC has experienced firsthand since 2014***, SchoolMessenger offers tight data integration with a wide variety of Student Information Systems (SIS) – ***including Banner***, Human Resource Systems, Point of Sale Systems, Transportation Systems, and even college-developed database applications. This is because over SchoolMessenger's long history, we have developed partnerships with most vendors of these systems, so that our integration and automation is both effective and smooth. Plus, the solution uses open standards so that the college can integrate SchoolMessenger with both off-the-shelf and customized applications.

Through the use of industry technologies and standards such as ODBC, CSV, XML, SFTP, Java, PHP, and SSL, SchoolMessenger is able to automate data integration in a flexible and secure manner with any database platform that supports external connectivity. Common examples of such database platforms include Oracle, Microsoft SQL Server, MySQL, PGSQL, and Microsoft Access (.mdb).

Updates can be:

- **Transaction based** – flagging specific students as absent today; and,
- **Demographic** – updating all phone numbers and grade level details for every student through unlimited updates.

During implementation, SchoolMessenger will configure its updating mechanisms to meet the college's specific needs.



Ability to upload users and criteria into system

✓ Yes. The system complies with this requirement in full.

Ability to post to social media applications and RSS feeds

✓ SchoolMessenger rapidly delivers to social media sites like Facebook and Twitter. Plus, SchoolMessenger directly updates RSS feeds.

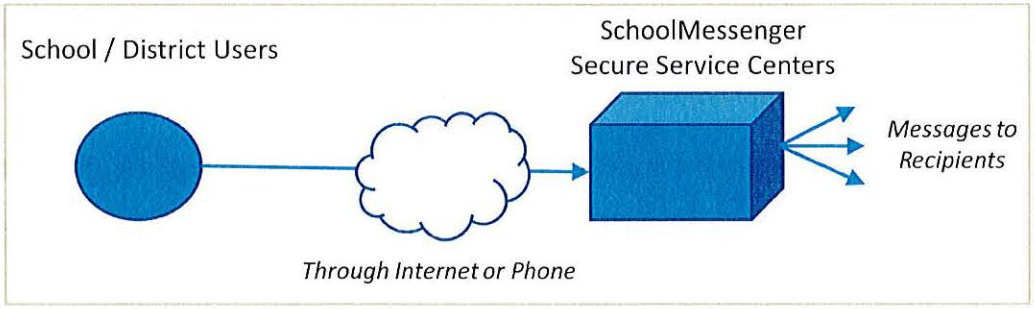
Ability to connect to LCD screens

✓ Yes. Provided the LCD screens can ingest RSS feeds, the system can post to LCD screens. Further, digital displays can receive and show SchoolMessenger notifications using SchoolMessenger's included Desktop Alerts software.

Emergency and non-emergency message hosted off site

✓ Yes. SchoolMessenger Communicate is fully web-based, and the configuration proposed here is the pure Software-as-a-Service (SaaS) model in which Intrado own and operate the entire infrastructure including hosting and phone lines. No hardware, software, plug-ins, phone lines, or infrastructure is required on the part of the College (other than using a computer or smartphone to access the internet). This model provides SCCC with:

- Access from any internet enabled device or telephone without any dependency on college technologies or resources;
- Rapid broadcast over our world-class infrastructure and patented distribution technology; and,
- Uptime, reliability, and capacity that comes from tens of millions of dollars of investment.



System shall be able to connect to College's active directory for authentication and LDAP

✓ Yes. With SchoolMessenger's LDAP integration, a Java-based client is installed on a college provided server (this could be a Virtual Machine, often the same one that is used for transferring data). It connects outbound to SchoolMessenger's servers using 256-bit SSL encryption. That connection is then used for a reverse proxy connection to perform authentication against the college's Active Directory servers. This approach eliminates the need for a college to open a port on their firewall to allow LDAP/AD connections. No

special groups are necessary; however, the usernames must match between SchoolMessenger and your AD environment. Active Directory integration is strictly used for name/password authentication.

CAS certified

✓ SchoolMessenger maintains all necessary certifications required for the performance of the functions specified under this RFP. Further clarification of this requirement is needed.

III. Implementation Schedule

The system shall be implemented and ready for use no later than February 24, 2020.

✓ Yes. ***We've served Suffolk County Community College with the exact notification services called for in this RFP since 2014.*** Upon award of the RFP, service will continue uninterrupted, but we'll evaluate your current use of the system to help make sure you're getting the most out of your investment. During implementation, we will:

- Identify additional data integrations available;
- Highlight popular features your users might not already be fully using;
- Supply refresher training; and,
- Ensure the system is fully ready to serve the College's notification needs.

As this would be a simple renewal, this would not need a full implementation; this entire process would involve only a few hours of the College's time.

IV. TRAINING

The Consultant shall provide training to College staff prior to the system being put into service, as well as ongoing training for new employees on an as-needed basis throughout the term of the Contract. Consultant shall provide all necessary audiovisual and printed materials, as well as instructors for this purpose. All capabilities and controls shall be demonstrated and all service requirements shall be reviewed during the training sessions.

Training

To ensure that Suffolk County Community College continues to get the most out of your investment, we are including ***unlimited web-based training for the life of the contract***. This includes user specific training, on-demand web-based based training, access to live weekly webinars, and access to our library of training videos and other instructional resources ***for ALL your staff, at no additional cost***.

Training Options

In practice, what this means is that we will tailor a fully custom training plan to meet the College's needs. We collaborate with your staff to determine the training program that best fits your objective, schedules, learning styles, and facilities. Options include:

- System Administrator training;
- Train the trainer training;
- End user training;
- Refresher training; and,
- Unlimited webinar training is available online at www.trainingschoolmessenger.com/.

On the following page, we've included a table that summarizes these options.

TRAINING FORMAT	DESCRIPTION	FACILITIES REQUIRED (ON SITE TRAINING)	FACILITIES REQUIRED (REMOTE TRAINING)	TYPICAL SESSION LENGTHS
System Administrator Training	Minimum level of training provided with every implementation. A small number of System Administrators – which may also include domain experts from data and networking – are trained on the management of the system or service. This training can be conducted either on site or remotely via a web meeting / conference call.	Office, conference room or computer lab with Internet access	Computer with Internet access Phone	90 minutes
Train-the-Trainers	The college may choose to have SchoolMessenger trainers work directly with designated college trainers. The training is designed to empower college trainers with the necessary confidence and skills to train	Computer lab with Internet access Data Projector	Computer lab Speaker Phone Data Projector	90 minutes

TRAINING FORMAT	DESCRIPTION	FACILITIES REQUIRED (ON SITE TRAINING)	FACILITIES REQUIRED (REMOTE TRAINING)	TYPICAL SESSION LENGTHS
	other end users throughout the college.			
End User Training	Typically performed "classroom style." Users need only attend one session and the training can be performed for as many individuals as the colleges's facilities will accommodate. Optionally, web-training sessions can be scheduled and attended by end users in dispersed locations via a web meeting / conference call. Distributed remote training sessions are limited to 999 participants per session.	Computer lab Data Projector	**Classroom style:** Computer lab Speaker Phone Data Projector **Dispersed Trainees:** Computer with Internet access Phone	45 - 60 min per session

TRAINING FORMAT	DESCRIPTION	FACILITIES REQUIRED (ON SITE TRAINING)	FACILITIES REQUIRED (REMOTE TRAINING)	TYPICAL SESSION LENGTHS
Refresher or Advanced Training	Similar to End User Training, follow-up training sessions are typically performed classroom style and can be done in remotely or on site.	Computer lab Data Projector	**Classroom style:** Computer lab Speaker Phone Data Projector **Dispersed Trainees:** Computer with Internet access Phone	45 - 60 min per session
Unlimited Webinar Training	New and advanced users can sign up for any of our webinar training sessions at their convenience. See what we have to offer at www.schoolmessenger.com/training. College-specific webinar trainings can also be arranged.	N/A	Computer with Internet access Phone	45 - 60 min per session

End-to-end process for certification and access

At the College's election, Intrado can oversee a process whereby end users must complete a live training session (online) prior to having their account activated. Intrado manages the complete end-to-end process and can optionally provide attendees with a certificate of completion.

Online Resources

In addition to embedded help and tutorials found within your solution, we also provide your users access to *Resource Central*, our rich customer resource and support website, which offers:

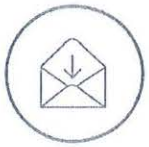
- Product News;
- Tips and tricks;
- Customer stories;
- Policy templates;
- System manuals;
- Training videos; and,
- Much more.

Experienced Trainers

We have invested significant resources in providing customers with a top-notch training experience. The dedicated training department holds several full-time trainers, each with significant professional development experience in the education sector.

V. CUSTOMER SERVICE

The Consultant shall be responsible for providing customer service to subscribers on an as-needed basis throughout the term of the Contract.



- ✓ Our products and services come with ***unlimited, 24/7/365 support – at no extra charge.*** There's no limit on the number of support cases you can submit and no cost for "premium" support. In addition, we never place restrictions on the number of people in your organization who can contact our support team. Any instructor, administrator, or support staffer can contact us anytime with questions on any type of issue.

  It should be noted, our unlimited, 24/7/365, support services are typically for any staff member of SCCC; as a practice, we do not provide support services to subscribers. However, we can easily assist your College and put together documentation and resources for your subscribers. And, if extending support services to your students is a condition of award, we can easily discuss an enhanced support package subject to an agreed upon annual fee.

UNDERSTANDING OF SERVICE REQUIREMENTS, MANAGEMENT TECHNIQUES AND APPROACH

Understanding of Service Requirements, Management Techniques and Approaches – Convey your understanding of the service requirements and demonstrate a thorough recognition of the services required under this RFP. This includes, but is not limited to, the following:

i. Summarize the implementation and service level approach, including:

1) Describe the implementation process. Identity the various considerations, approaches and strategies that will be utilized under this Agreement.

2) Articulate the staffing and time resources required on the College side, both functional and technical, required to implement your system based upon previous working groups.

✓ ***Intrado has served Suffolk County Community College continuously with the exact notification services called for in this RFP since 2014.*** Upon award of the RFP, service will continue uninterrupted, but we'll evaluate your current use of the system to help make sure you're getting the most out of your investment. During implementation, we will:

The same SchoolMessenger solution trusted by Suffolk County Community College to send over 3.59 Million notifications over the past 12 months!

- Identify additional data integrations available;
- Highlight popular features your users might not already be fully utilizing;
- Provide refresher training; and,
- Ensure the system is fully ready to serve the college's notification needs.

As this would be a simple renewal, this would not require a full implementation; this entire process would involve ***only a few hours of the college's time***.

3) Include information about service level agreement expectations, such as around-the-clock support (24/7/365), maximum length of downtime, upgrade intervals, etc. how long to reach certain number of people

✓ Yes. Intrado has complied with this requirement in full. Please see the following responses.

Support

Unlike some solutions, our products and services come with ***truly unlimited, 24/7/365 support – at no extra charge.*** There's no limit on the number of support cases you can submit and no cost for "premium" support. In addition, we never place restrictions on the number of people in your organization who can contact our support team. Any teacher, administrator, or support staff can contact us anytime with questions on any type of issue.

Support services are available through a toll-free 800 number, e-mail, live chat, and web-form for all users for all issue types ***at no additional cost.***

We are a recognized leader in ongoing support and customer service. Our customer care philosophy is based on friendliness, courtesy, and quick service. We go beyond traditional support and look for opportunities to ensure that end users are trained effectively and prepared to communicate meaningfully with their community.

Additionally, all Customer Service is:

- Supplied by the SchoolMessenger Customer Service Team (never subcontracted or outsourced);
- North American based; and,
- Designed for the unique needs of educators.

Downtime

SchoolMessenger Communicate is available 24/7/365. Communicate delivers a maximum uptime that historically exceeds 99.999%. We maintain multiple continuously synchronized data centers on distinct national power grids. These redundant datacenter facilities are in addition to multiple redundant connections to the nation's telephone network in multiple geo-dispersed cities. With this infrastructure and corresponding disaster recovery plan, we respond to any unforeseen unavailability with near instantaneous fail over.

Upgrade intervals

We are constantly improving our software. Major feature releases are scheduled every six months, and minor enhancements are scheduled every quarter. All of these features are built based on customer feedback and are ***free of charge***.

Listening to our customers has allowed SchoolMessenger to build a robust notification solution that is easy to use and easy to deploy. Through extensive customer surveys (web based, proactive phone calls, CRM logging), SchoolMessenger captures and analyzes customer feedback. This feedback is then evaluated again development priorities to ensure a product roadmap that is in line with customer needs.

As evidence of SchoolMessenger's ongoing commitment to research and development, note that over the past few years, the company has launched several major updates. Significant updates include:

- Brand new message sender;
- Desktop alerts;
- Email tracking with Read Duration Reporting;
- Email stationery system;
- Mobile sender apps;
- Broadcast templates;
- Additional language translations;

- Enhanced preference control;
- Two-Way messaging;
- Much more.

Each update was delivered in a manner to minimize disruption for end users, with many upgrades being optional and at the College's election. Every update is delivered at no additional cost.

Speed of Delivery

Large schools, districts, colleges, and education entities across the United States and Canada, including New York City Schools, with a student population of over 1 Million students, and Toronto District School Board with over 275,000 students, have selected Intrado's SchoolMessenger solution because of our ability to deliver rapid notifications to their recipients.

We routinely deliver hundreds of thousands of messages in minutes, is well contracted with carriers to exceed the delivery requirements of our aggregate customer base and has numerous actual documented examples in the one million messages per hour range.

We commend SCCC's commitment to thoroughly researching vendors' ability to initiate and deliver large volumes of calls. The best evidence to support this capability is actual performance in North America's largest school systems, something that is only proven in a small number of top tier notification providers. We:

- Serve more K-12 and education sector enrollment than any other single notification service;
- Serve more large urban school systems than any other single notification service;
- Are trusted by 3 branches of US Military and numerous first responders; and,
- On average use less than 2% of its available capacity.

Due to variables outside our control (i.e. the capacity of the local phone exchange in the greater metropolitan area), we do not state theoretical guarantees such as "initiate X

million calls per hour." We can confirm that thanks to our contracted capacity, delivery algorithms, and multiple telecom partnerships we generally deliver notifications as fast as the local area can accept incoming calls.

Below are delivery rate statistics from actual broadcasts sent by other large education institutions:

VOICE MESSAGES	SMS TEXT MESSAGES	EMAIL MESSAGES
250,000 calls = approx. 15 minutes	250,000 messages = approx. 10 minutes	250,000 emails = approx. 5 minutes

In addition, please consider the following examples of extremely large volumes of notifications sent through the same service proposed here:

- Over 3 Billion messages in 2018;
- 23.5 Million phone messages during Hurricane Florence (Sept. 12-17, 2018);
- 29.4 Million phone messages during Hurricane Harvey (August 23-31, 2017);
- 15.3 Million in 18-hour period dubbed the "polar vortex" (January 21, 2014);
- 25.1 Million over 2 days of Superstorm Sandy (October 2012); and,
- 14 Million in 24-hour period of ice and snow (February 1-2, 2011).

US Patent No. 8131269

Our system uses geo-dispersion technology that allows the industry-leading hosted notification solution to achieve near-infinite scalability and an unmatched level of redundancy and performance. In fact, we were awarded a patent (***U.S. Pat. No. 8,131,269***) for our highly available, distributed notification technology architecture. The patented technology prepares voice messages and delivers them in mass, to a single recipient, or to a

particular group or household, ***more quickly and with a higher degree of redundancy than earlier generation architectures.*** It also provides the intelligence necessary to allocate those messages across its highly distributed infrastructure, increasing the overall redundancy and resiliency of the system. The basis of the patent is a system and method, which uses a highly distributed architecture to deliver extremely large volumes of mass notifications originating from many locations nearly instantaneously.

Congestion Management

We consistently contact large audiences very quickly; however, if the area receiving the calls can't handle all those calls, sending them at once will only overwhelm the phone network. That's why our platform utilizes a unique Congestion Management Algorithm to maximize call delivery. Calls are delivered into any geographic area without overloading the local telecom infrastructure. This means your notification goes out efficiently and effectively.

4) Demonstrate adequate facilities and resources to deliver messaging and redundancy through the system

- ✓ All components of the application reside in multiple geo-dispersed datacenters (all SAS 70 Type II certified). Plus, it has redundant connections to the telephone grid. And, information is synchronized at every location. This means that even in the unprecedented case of a regional event affecting any part of the country, servers at the other locations continue processing notifications without interruption.

  Moreover, our massive capacity allows users to send hundreds of thousands of calls in minutes. On average, we utilize less than 2% of our available capacity, and grow this capacity as needed based on usage. This helps ensure that during periods of peak activity (or even a regional emergency) the service can handle the needs of SCCC.

5) Proposals shall include a detailed description, including contact information for customer service by the subscribers and how the Contractor will work with subscribers to resolve any potential problems they may have with using the system.

✓ Unlike some solutions, our products and services come with truly unlimited, 24/7/365 support – ***at no extra charge.*** There's no limit on the number of support cases you can submit and no cost for "premium" support. In addition, we never place restrictions on the number of people in your organization who can contact our support team. Any teacher, administrator, or support staff can contact us anytime with questions on any type of issue.

Support services are available through a toll-free 800 number (1-800-920-3897), e-mail (support@schoolmessenger.com), live chat, and web-form for all users for all issue types at no additional cost.

Additionally, all Customer Service is:

- And, because getting help quickly is often a requirement, we o Supplied by the SchoolMessenger Customer Service Team (never subcontracted or outsourced);
- North American based; and,
- Designed for the unique needs of educators.

It should be noted, our unlimited, 24/7/365, support services are typically for any staff member of SCCC; as a practice, we do not provide support services to subscribers. However, we can easily assist your College and put together documentation and resources for your subscribers. And, if extending support services to your students is a condition of award, we can easily discuss an enhanced support package subject to an agreed upon annual fee.

6) Describe the level of continual two-way communication you will maintain with College administrators.

✓ Yes. We provide each customer with a dedicated Account Manager for rapid resolution of any issue that may arise. Mr. Bill Tribout, Account Development Services Manager will continue to serve SCCC. Mr. Tribout will be responsible for ensuring the College's goals are being met, coordinating training, and serving as application specialist and primary point of contact. Contact information follows:

ACCOUNT DEVELOPMENT MANAGER AND ACCOUNT LEAD FOR SCCC

Bill Tribout, Account Development Services Manager
1-888-527-5225 ext. 1622 (desk)
1-800-360-7732 (fax)
btribout@intrado.com

ii. Provide a timeline and schedule for the installation, set-up, and implementation of the system in accordance with the requirements set forth in Section III –Scope of Work.

✓ ***Not applicable. As noted in our above response, Intrado has served Suffolk County Community College continuously with the exact notification services called for in this RFP since 2014.*** Upon award of the RFP, service will continue uninterrupted, but we'll evaluate your current use of the system to help make sure you're getting the most out of your investment. As this would be a simple renewal, this would not require a full implementation; this entire process would involve ***only a few hours of the College's time.***

The same SchoolMessenger solution trusted by Suffolk County Community College to send over 3.59 Million notifications over the past 12 months!

iii. Additional Features - Describe any additional features of your system. Provide suggestions for additional electronic communication systems or solutions that may be of benefit to the College.

✓ ***SchoolMessenger solutions are the trusted platform for school community engagement.*** We provide a wide range of communication solutions each expertly crafted to meet the unique needs of educators. Moreover, all of which are designed to easily integrate with each other – so even though our products are powerful on their own, they're even better together. Here are three examples that may be of interest to the College. Optional pricing can easily be provided upon request.

SCHOOLMESSENGER PRODUCTS AND SERVICES:		
☐	 **SchoolMessenger CustomApp**	• Delivers key college content to students, staff, and the community on the go. • Truly custom app that integrates all communications – from the website, notification service, and other sources. • Trusted by more than 1,000 schools, districts, and education institutions.
☐	 **SchoolMessenger K-12 Social**	• Complete social media solution for institutions. • Publish across social networks, listen to conversations, and analyze performance all from a single platform. • Improve community engagement.

SCHOOLMESSENGER PRODUCTS AND SERVICES:

☐	**SchoolMessenger SecureFile**	• Add-on to SchoolMessenger Communicate • Send virtually any document or file securely. • Report cards, test scores, payment slips, and more can be safely delivered, while reducing printing costs. • Reporting and tracking makes document management a breeze.

iv. Training and Support - Describe the training approach at the time of implementation and subsequent training support that will be provided throughout the term of the Agreement. Include information regarding long term training support and staffing available for on-going training as needed. Clearly indicate whether training sessions will be offered on-site, remotely or a combination of both.

- ✓ As noted in more detail in our above responses, to ensure that Suffolk County Community College continues to get the most out of their investment, we are including ***unlimited remote web-based training for the life of the contract.*** This includes user specific training, on-demand web-based based training, access to live weekly webinars, and access to our library of training videos and other instructional resources ***for ALL your staff, at no additional cost.***

[PAGE INTENTIONALLY LEFT BLANK]

b) Understanding of System Requirements and Submission of VPAT

Submission of VPAT – Proposers shall submit a completed VPAT with properly documented exceptions, if any, as well as a roadmap for compliance in accordance with Section 508 of the Rehabilitation Act of 1974 and subsequent updated requirements. v More information on the VPAT as well as a template can be found here: https://www.section508.gov/sell/vpat

i. Proposer shall demonstrate that all portal interfaces meets ADA Compliant Guidelines as described in Section I – Administrative Information, Sub-section 11 – RFP Policies and Procedures.

- ✓ The accessibility of our products and services to people with disabilities is very important to Intrado. Of course, accessibility depends on a combination of our platform, institution sender practices, and the message recipient's device and expressed preferences. SchoolMessenger Communicate includes the ability for our customers to customize the administrative and user settings in order to personalize messages to recipients in a format that is most accessible to their needs. Specifically, SchoolMessenger Communicate allows for institutions to create and disseminate content via a number of channels: voice, email (plain text and HTML), SMS text, RSS, and social media. In addition, we provide system administrators with a number of controls to force content creation by channel, assuring recipients with disabilities can consume content in their preferred format.

  This sender functionality is further complemented and enhanced by options for message recipients, who have the ability to choose the best way to receive their notifications, on the device they want, regardless of how it is sent. For example, if a notification is sent as just a phone call, recipients can choose to receive that phone call as a link in an email or a link in a text message. These user preferences support accessibility by engaging recipients who may not be able to hear audio messages, or may not be able to view text-based messages, so that they can receive the message automatically in a medium and format they prefer.

  Recipients can also use the accessibility options built into modern cellular devices such as screen readers and magnification to receive emails and text messages in an accessible format. Many browsers and operating systems have similar assistive technology tools to support accessibility on the recipient side. Our notifications can also take advantage of

push notifications directly to the cellular device, thus further taking advantage of those accessibility features.

c) Higher Education Cloud Vendor Assessment Tool (HECVAT – Full Version) (applicable for Cloud Computing Software)

Higher Education Cloud Vendor Assessment Tool (HECVAT) for Cloud-Hosted Services – The College requires Proposers that provide cloud-hosted services to complete a full Higher Education Cloud Vendor Assessment Tool (HECVAT). Proposers including a cloud-hosted solution shall complete and submit with their proposal, the HECVAT Full Version which can be accessed through the following link: https://www.ren-isac.net/public-resources/hecvat.html

- ✓ Many of your questions ask for full security policy and procedure documents to supplement the responses. At Intrado, we see privacy and security as paramount. We also see the confidentiality of our practices and procedures as essential to maintaining information security and the trust placed in us by our many clients. Accordingly, we've provided high-level responses and a few attachments to supplement the following table. If full policy documents are required as a condition of award, we can easily provide additional information under a non-disclosure agreement.

Higher Education Community Vendor Assessment Tool (HECVAT) - Full

Version 2.10

HEISC Shared Assessments Working Group

DATE-01	**Date**	*12-6-2019*

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Community Vendor Assessment Toolkit (HECVAT). Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by Institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with Institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor. Review the *Instructions* tab for further guidance.

GNRL-01 through GNRL-08; populated by the Vendor

GNRL-01	Vendor Name	*Intrado Interactive Services Corporation*
GNRL-02	Product Name	*SchoolMessenger Communicate*
GNRL-03	Product Description	*SchoolMessenger Communicate, our mass notification system, provides rapid, reliable, and secure multi-channel notifications.*
GNRL-04	Web Link to Product Privacy Notice	*https://www.schoolmessenger.com/privacy-statement and https://www.west.com/legal-privacy/*
GNRL-05	Vendor Contact Name	*Nate Brogan*
GNRL-06	Vendor Contact Title	*President, Notification Services*

GNRL-07	Vendor Contact Email	nkbrogan@west.com
GNRL-08	Vendor Contact Phone Number	*1-888-527-5225 ext. 201*
GNRL-09	Vendor Data Zone	*Our notification products and services are available across North America. For the purpose of clarity, this self-assessment and all answers provided are based on the US-based deployment currently in place for the Suffolk County Community College. And, in this model, all data resides in the United States.*
GNRL-10	Institution Data Zone	*The United States.*
GNRL-11 and GNRL-12; populated by the Institution's Security Office		
GNRL-11	Institution's Security Analyst/Engineer	*Information Security Office*
GNRL-12	Assessment Contact	infosec@intrado.com

Instructions

Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 3:** Submit the completed Higher Education Community Vendor Assessment Toolkit (HECVAT) to the Institution according to institutional procedures.

Qualifiers	Vendor Answers	Additional Information	Guidance
The institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. **Responses to the following questions will determine the need to answer additional questions below.**			

QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	No	No. The product being proposed does not process or store protected health information.	Responses to the questions in the HIPAA section are optional.
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	Yes	Yes. The SchoolMessenger Communicate application includes a mobile app for recipients and a mobile app for administrators to rapidly initiate messages.	You are required to complete the questions in the Mobile Application section.
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	Yes	Yes. We collocate in our own instance within the Amazon Cloud.	You are required to complete the questions in the Third Parties section.

QUAL-04	Do you have a Business Continuity Plan (BCP)?	Yes	Intrado has established a rich framework for both Business Continuity and Disaster Recovery Planning. Business Continuity addresses the sustainment of business operations in the context of a comprehensive approach to include migration strategies, capabilities, and processes. The Disaster Recovery Plan outlines the processes by which the business will resume after a disruptive event such as an earthquake, flood, or even a virus attack. These plans are communicated, exercised, maintained, and refreshed on a periodic basis. At a high level, these plans include the following: The Business Continuity Framework contemplates: • Mitigation Strategy o Carrier Grade Data Center environment o Periodic exercise of back up and service restoration processes o Complete Data and Application back up processes § Scheduled images § Off-site storage and retention policies • Communication Planning o Internal communications (operational issues, escalations, status reporting) o Customer contacts and notification procedures o Vendor and supplier contacts • Incident Assessment and Planning o Environmental Disasters	You are required to complete the questions in the Business Continuity section.

			o Organized or Deliberate Disruptions o Loss of Utilities and Services (including Network) o Equipment or System failures o Security Incidents • Business Risk Assessment o Key Business Processes o Financial risk mitigation and management plan • Backup and recovery strategies o Alternative Business Process Handling o Systems backup and recovery o Customer Service o Administration and Operations o Training and mock exercises • Key Personnel o Disaster Recovery Team o Business Recovery Team o Staff Plan	
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	Yes	We maintain full disaster recovery plans. Critical data is replicated in multiple data centers. And, we offer a typical recovery time objective of 15-30 minutes in the event of a catastrophic system failure.	You are required to complete the questions in the Disaster Recovery section.
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	No	No. The system does not process or store credit card or any other data governed by PCI DSS.	Responses to the questions in the PCI DSS section are optional.

QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	No	Intrado is a consultant providing a Software-as-a-Service.	Responses to the questions in the Consulting section are optional.
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**
DOCU-01	Have you undergone a SSAE 16 audit?	Yes	The data centers we collocate within are subject to SOC 2, Type 2 audits. For a copy of the SOC 3, please see immediately following this table.	Provide the date of assessment and include a SOC 2 Type 2 (preferred) or SOC 3 report. If you have a SOC3 report, include a URL for the published report. Indicate if your hosting provider was the subject of the audit.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	No	To date, we have not completed a Cloud Security Alliance self assessment in relation to this product.	Describe any plans to complete the CSA self assessment or CAIQ.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	We are constantly monitoring security and certification standards in relation to our products and services, as well as industry best practices. At this time, we have no firm plans to embark on a Cloud Security Alliance STAR certification, as that certification is predominantly focused on GDPR regulations that govern data collocated in Europe, whereas the specific application being proposed is collocated exclusively in the United States.	Describe any plans to obtain CSA STAR certification.

DOCU -04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)	Yes	Yes. We have an extensive security framework, with the standards varying based on the area of security. Here are a few examples: Our data center is ISO 27001 and SSAE 16 certified . Our information security practices and procedures are created to align with ISO 27002 and NIST. And, our data destruction aligns with DoD standards. If there is a specific area of our practices and procedures that are of concern, please let us know and additional supporting documentation can easily be provided.	Provide documentation on how your organization conforms to each framework and indicate current certification levels, where appropriate.
DOCU -05	Are you compliant with FISMA standards?	No	The data centers that house our data are FISMA compliant. At this point, the application has not been certified for compliance.	Describe any plans to become FISMA compliant.
DOCU -06	Does your organization have a data privacy policy?	Yes	Yes. Policy statements can be viewed at: https://www.schoolmessenger.com/privacy-statement and https://www.west.com/legal-privacy/. If more detailed policies are required, they can easily be provided under a non-disclosure agreement.	Provide your data privacy document (or a valid link to it) upon submission.
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**

COMP -01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	SchoolMessenger is part of Intrado Corporation (formerly known as "West Corporation"), a privately-owned corporation and one of the world's largest communication companies. For more than 25 years, Intrado has provided reliable, high-quality voice and data services. Intrado serves clients in a variety of industries including telecommunications, public safety, technology, healthcare, financial services, and retail. Intrado operates worldwide, in the United States, Canada, and many other countries. And, Intrado manages more than 90% of the United States' emergency 911 systems, owns and operates approximately 750,000 telecom ports and provides tremendous scale, stability, and resources.		Include circumstances that may involve off-shoring or multi-national agreements.
COMP -02	Describe how long your organization has conducted business in this product area.	SchoolMessenger notification services have been sold since 1999.		Include the number of years and in what capacity.
COMP -03	Do you have existing higher education customers?	Yes	At Intrado, we treat our commitment to maintaining our clients' confidentiality and privacy as paramount. Just as we would never disclose your contract details without your consent, we do not disclose full client listings of such information in RFP responses. We can confirm that we serve over 10,500 customers comprising thousands of schools, districts, and education organizations. We can also confirm that we serve over 65 higher education entities with the product proposed in this RFP response. The success of SchoolMessenger's products and services is further evidenced by the company's many references from large	Provide a list of Higher Ed references, with contact information.

			education organizations, zero cancellation on-boarding rate, and net renewal rate of 97%.	
COMP -04	Have you had a significant breach in the last 5 years?	No	We have never experienced a security breach.	
COMP -05	Do you have a dedicated Information Security staff or office?	Yes	Yes. Ben Smith, EVP Information Security is responsible for Intrado's information security. And, Mr. Smith maintains a full InfoSec office whose sole focus is our information security policies, procedures, practices, and continuous staff training. This includes over 65 full-time employees exclusively focused on information security, with positions and title including analysts (such as mining analysts, business analysts, software analysts), project managers, facilities/property management experts, information security managers, and attorneys.	Decribe your Information Security Office, including size, talents, resources, etc.

COMP -06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	Yes. Exact staffing breakdown is confidential, but we can confirm that we have fully separated teams for all these functions and have well over 150 employees dedicated to the SchoolMessenger products and services.	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)
COMP -07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	Please see the attached "Hosting, Security, and Privacy" for additional supporting detail.		Share any details that would help information security analysts assess your product.
Third Parties		**Vendor Answers**	**Additional Information**	**Guidance**
THRD -01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service	All third-party companies are fully vetted by our Information Security team and only allowed to be used if they satisfy their security assessment, sign all the appropriate contracts, and commit to our requisite non-disclosure agreements. If additional details are needed on our vetting procedures and contracts, this can easily be provided under a non-disclosure agreement.		Ensure that all elements of THRD-01 are clearly stated in your response.

	recoverability, and confidentiality.		
THRD -02	Provide a brief description for why each of these third parties will have access to institution data.	The third party that would potentially have access to the institutions data would be our hosting provider, Amazon. As noted above, this relationship is governed by a formalized contractual relationship.	If more space is needed to sufficiently answer this question, provide reference to the document or add it as an appendix.
THRD -03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	All third-party arrangements are governed by formal contracts and non-disclosure agreements.	Provide sufficient detail for each legal agreement in place.
THRD -04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	This information can easily be provided under a non-disclosure agreement.	Robust answers from the vendor improve the quality and efficiency of the security assessment process.

Consulting - Optional based on QUALIFIER response.		Vendor Answers	Additional Information	Guidance
CONS-01	Will the consulting take place on-premises?	No	No. The proposed solution is a pure SaaS deployment.	
CONS-02	Will the consultant require access to Institution's network resources?	No		
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	No		
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	No		
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	Yes	All employees at Intrado are subject to annual retraining on sensitive data handling. Examples include but are not limited to: Incident Response Plan (IRP) training, GDPR Compliance Training, HIPAA Compliance Training, Security Awareness Training, Global Privacy Training, Telephone Consumer Protection Act (TCPA) training, CPNI Training, and many more.	State the name of the training received and the most currently training date for each training.

CONS-06	Will any data be transferred to the consultant's possession?	Yes	SchoolMessenger Communicate requires minimal data fields in order to send targeted notifications. The minimum required fields are first name, last name, student ID, and campus location. All data transmissions are encrypted in transit (via 256 SSL) and encrypted at rest (via an AES cipher).	State how long the data will remain in their possession and state how the data will be protected.
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	Yes	All data within the application is encrypted at rest using an AES encryption cipher.	Describe how encryption is implemented.
CONS-08	Will the consultant need remote access to the Institution's network or systems?	No		
	Can we restrict that access based on source IP address?			
Application/Service Security		**Vendor Answers**	Additional Information	**Guidance**
APPL-01	Do you support role-based access control (RBAC) for end-users?	Yes	Institution-definable access profiles can be created for role-based user access.	Describe any infrastructure dependencies.
APPL-02	Do you support role-based access control (RBAC) for system administrators?	Yes	Institution-definable access profiles can be created for role-based user access.	Describe the utilized technology.

APPL-03	Can employees access customer data remotely?	Yes	As the application is a cloud-hosted SaaS platform, certain employees can access customer data remotely, but only via secure VPN tunnel.	If available, submit documentation and/or web resources.
APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	Yes	A high-level diagram has been included in the attachment "System Architecture" immediately following this table. If more detailed diagrams are required, this can easily be disclosed under a non-disclosure agreement.	Provide a reference to the requested documents or provide them when submitting this fully-populated HECVAT.
APPL-05	Does the system provide data input validation and error messages?	Yes		Provide a reference to documentation of your data input validation and error messaging capabilities.
APPL-06	Do you employ a single-tenant environment?	No	The application/environment is multi-tenant, but all customer databases are single-tenant.	
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	Not applicable. The proposed solution is a Software-as-a-Service deployment and is operating system independent and fully browser-based.		List all operating systems and the roles that are fulfilled by each.
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	No		

APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	A system of record for data that is sent to the application is required. Typically, this is a Student Information System, and/or HR system managed by the Customer, but could be as simple as a spreadsheet.		Describe the products and how they will be implemented.
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	Please see the attached "Hosting, Security, and Privacy." If a higher level of detail is required, we can easily provide such information under a non-disclosure agreement.		Ensure that all parts of APPL-10 are clearly stated in your response. Submit architecture diagrams along with this fully-populated HECVAT.
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	Yes	Application front-ends (webs) and backend databases are segregated from one another.	Provide a brief description.
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	The proposed solution is deployed as a Software-as-a-Service with the interface being fully browser-based. As such, all aspects of the solution are accessible via a web-based interface. For a solution overview summarizing the platform features and tools, please see section "IV. Technical Proposal" within the core RFP response document.		Include both end-user and administrative features and functions.

APPL-13	Are there any OS and/or web-browser combinations that are <u>not</u> currently supported?	Yes	The system is web-based and platform independent. It is compatible with commonly used web browsers including mobile web browsers. For optimal performance, we recommend the following web browsers: • Internet Explorer 11+; • Google Chrome 65+; • Microsoft Edge 16+; • Mozilla Firefox 64+; and, • Safari 11+.	Describe all OS and web-browser combonations that are not currently supported.
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?	Yes	While the platform does provide the ability to use mobile applications for sending notifications, as well as for recipients to modify contact preferences, location data is not stored/tracked.	Provide a detailed description of system capabilities and how location data is secured.
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	From an end-user standpoint, the system's security profile model allows the College to determine levels of access. With regard to security and administration functions within Intrado, access is strictly controlled and monitored.		Include a detailed description of how security administration and system administration authority is separated, controls are verified, and logs are reviewed regularly to ensure appropriate use.
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	Administrator access is granted to specific access profiles, and only users with that profile have access to those administrative functions. The principal of least privilege can be enforced through the access profile, while provisioning and deprovisioning of administrator accounts is handled in the user interface by designated administrator users.		Ensure that all parts of APPL-16 are clearly stated in your response.

APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).	We are redundantly collocated in different clouds and zones of availability throughout the United States. Please see attachment "Hosting, Security, and Privacy" for supporting detail on how our system is configured with zero points of failure.	Ensure that all parts of APPL-18 are clearly stated in your response. The examples given are not exhaustive - elaborate as necessary.
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**
AAAI-01	Can you enforce password/passphrase aging requirements?	No	The system does not have a framework for aging passwords and password history, as the system does not store users' credentials. Specifically, all credentials are subject to a salted hash encryption at the point of authentication and are never stored in plain text. Moreover, to date, we've shied away from implementing an aging policy because much of the industry literature suggests that aging requirements actually increase risk.	Describe plans to support password/passphrase aging requirements.

AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes	The application's password policy is highly configurable. The district may determine its own length rules for usernames and passwords, as well as configure lockout rules based on invalid password attempts (including the maximum number of invalid log-in attempts, the number of minutes a user is temporarily locked out before they can try again, and whether repeated invalid log in attempts will trigger the disabling of an account). In addition, to maintain a high level of authentication integrity, the application enforces a policy to automatically prevent users from creating passwords that are easily guessed (e.g. too similar to the username, or lacking a combination of letters / numbers, etc.).	Describe how password/passphrase complexity requirements are implemented in the product.
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?	Yes	As noted in more detail in our previous response, the password policies are configurable by the college.	Describe these limitations and/or restrictions and state what lengths and complexities are supported.
AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	Yes	The college can determine its own reset procedures.	Describe your documented password/passphrase reset procedures that are currently implemented in the system and/or customer support.

AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	Yes	The system supports authentication via LDAP and SAML, as well as direct log in access.	Describe or provide a reference to the supported types of authentication.
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?	No	SchoolMessenger stores all passwords using an irreversible one-way hash algorithm. Passwords can be verified but can never be read. This is a distinct security advantage over applications which store passwords using only two-way encryption, or simply store them as plain-text (where anyone with direct access to the database could also have access to passwords).	
AAAI-07	Are user account passwords/passphrases visible in administration modules?	No	No. See previous response for supporting detail.	
AAAI-08	Are user account passwords/passphrases stored encrypted?	Yes	SchoolMessenger stores all passwords using an irreversible one-way hash algorithm. Passwords can be verified but can never be read.	Describe or provide a reference to the algorithm/strategy that is used to encrypt stored passwords/passphrases.
AAAI-09	Does your *application* and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google	No	At this time, we have no plans to include multi-factor authentication. We are constantly monitoring security standards and best practices to ensure that our solutions meet the needs of our clients. In addition, our development work is often	Describe any plans to support multi-factor authentication in your application.

	Authenticator, OTP, etc.)		driven by customer requests; at this time, this is not a frequently requested item.	
AAAI-10	Does your *application* support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?	Yes	The system supports authentication via LDAP and SAML, as well as direct log in access.	Provide a brief description of supported authentication and authorization systems.
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	No		
AAAI-12	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	Yes	The system supports authentication via LDAP and SAML, as well as direct log in access.	Describe all authentication services supported by the system.
AAAI-13	Does the system operate in a mixed authentication mode	Yes	Yes. The system will support either or a combination thereof.	Provide a detailed description of your mixed authentication mode practices.

	(i.e. external and local authentication)?			
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?	No		
AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	The platform is equipped with detailed reports that capture key audit details such as all login/logout data, all locked user accounts (such as accounts where access has been frozen due to repeated access attempts using an incorrect password), all banned user accounts, and other key information associated with activity within the platform.	Ensure that all elements of AAAI-15 are evaluated for your response. Provide a description of logging capabilities.
AAAI-16	Describe or provide a reference to the a) system capability to **log** security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to	The application logs are only accessed by Intrado's staff. The application logs contain the change, date, time, nature of event, and seriousness of event violation. In addition, the platform is equipped with detailed reports that capture key audit details such as all login/logout data, all locked user accounts (such as accounts where access has been frozen due to repeated access attempts using an incorrect password), all banned user accounts, and other key information associated with activity within the platform. With regard to logging changes to privileges, the system does not explicitly log these changes; however, these changes are tracked and can be back traced through the web access logs and data replication logs.		Ensure that all elements of AAAI-16 are clearly stated in your response.

	implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.		
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	Logs are retained for the life of the contract and are accessible only by Intrado's team.	Ensure that all elements of AAAI-17 are clearly stated in your response.

Business Continuity Plan		Vendor Answers	Additional Information	Guidance
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	It's Intrado's policy not to disclose business continuity and disaster recovery plans without an executive non-disclosure agreement. Accordingly, while we've answered yes or no to the following questions, supporting documentation will not be furnished at this time.		Provide a valid URL to your current BCP or submit it along with this fully-populated HECVAT.
BCPL-02	May the Institution review your BCP and supporting documentation?	Yes		Provide a reference to your BCP and supporting documentation or submit it along with this fully-populated HECVAT.

BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	Yes		Provide additional details, as needed.
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Yes		Summarize your defined problem/issue escalation plan contained in your BCP.
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	Yes		Summarize your documented communication plan contained in your BCP.
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes		Describe your BCP component review strategy.
BCPL-07	Has your BCP been tested in the last year?	Yes		State the date of your last BCP test.
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	Yes		Describe your training and awareness activities.
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	Yes		Summarize these crisis management roles and responsibilities.

BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	Yes		Provide the distance (in miles) between the primary and secondary locations.
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Yes		State the date of your last alternate site relocation test.
BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	Yes		Provide a brief summary to support your selection.
Change Management		**Vendor Answers**	**Additional Information**	**Guidance**
CHNG-01	Do you have a documented and currently followed change management process (CMP)?	Yes	Impact analysis is performed and risks are identified prior to any change. Changes must be authorized by multiple designated approvers on different teams/disciplines. All changes are made first in a testing/staging environment and tested to ensure functionality. Only approved IT staff have the ability to make changes to the production environment.	
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately	Impact analysis is performed, and risks are identified prior to any change. Changes must be authorized by multiple designated approvers on different teams/disciplines. All changes are made first in a testing/staging environment and tested to ensure functionality. Only approved IT staff have the ability to make changes to the production environment.		Ensure that all parts of CHNG-02 are clearly stated in your response.

	authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.			
CHNG -03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	Yes	Major platform changes that could impact security are rare but would be notified at least 30 days in advance. Typically, these changes/features would be opt-in rather than opt-out, unless regulation or legal reasons require it.	State how and when the Institution will be notified of major changes to your environment.
CHNG -04	Do clients have the option to not participate in or postpone an upgrade to a new release?	No	As a SaaS platform, release updates are performed system wide.	Summarize why clients do not have alternative release option.
CHNG -05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	As a SaaS platform, all customers are running the latest version of the software. Concurrent versions are not supported.		Ensure that all relevant details pertaining to CHNG-05 are clearly stated in your response.

CHNG -06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	All customers are on the most recent version of the software. Software "versions" are not published.		Ensure that all parts of CHNG-06 are clearly stated in your response.
CHNG -07	Does the system support client customizations from one release to another?	No	Not applicable. The proposed solution is an out-of-the-box platform designed to natively support client-based configuration is tailored to meet each client's needs. That being, the client	Describe any business or technical reasons why customizations are not supported.
CHNG -08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	Yes	All potential updates/releases go through multiple levels of code review, Quality Analysis testing, and QA validation through documented test cases in test environments prior to being placed into production, as well as after being placed into production.	Describe how this is accomplished within your environment.

CHNG -09	Do you have a release schedule for product updates?	Yes	Major feature releases are scheduled every six months, and minor enhancements are scheduled every quarter. Hotfixes or patches are released as required, typically during the scheduled maintenance window. The maintenance window is one Friday night per month from 11 PM – 2 AM Eastern Time. Note that although this window is available monthly, it is only used approximately twice per quarter.	Provide a reference to this product's release schedule.
CHNG -10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?	Yes	As a standard practice, we don't disclose full product roadmap details as part of the RFP process. We can confirm that we provide quarterly updates and enhancements and that we constantly refine our roadmap based on customer feedback and communication trends.	Provide a reference to your technology roadmap.
CHNG -11	Is Institution involvement (i.e. technically or organizationally) required during product updates?	No		
CHNG -12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Yes	Yes. The platform is constantly monitored for vulnerabilities and patches are evaluated within 30 days of release. However, deployment schedules vary based on testing and our ability to confirm stability prior to deployment. Where possible, patches and software updates are performed during our standard maintenance window. When patches and updates are deemed	Summarize the policy and procedure(s) managing how critical patches are applied to systems and applications.

			essential, emergency maintenance is ordered, and it occurs outside of standard business hours.	
CHNG -13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	This information can not be disclosed without a signed Non-disclosure agreement.	Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.
CHNG -14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes	Yes. Updates are performed silently and transparently to end users by our team after an extensive quality assurance process. Each update is delivered in a manner to minimize disruption for end users, with many upgrades being optional and at the College's election. And, the district will be notified by email and/or phone call in advance of any updates.	Define current off-peak hours.
CHNG -15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	Yes	All emergency changes (hotfixes) follow the same change management procedures in place for regular releases, including the same level of testing/QA in pre-production environments prior to being placed into production.	Summarize implemented procedures ensuring that emergency changes are documented and authorized.

Data		Vendor Answers	Additional Information	Guidance
DATA-01	Do you physically and logically separate Institution's data from that of other customers?	Yes	SchoolMessenger separates all customer data into separate logical secure database partitions. Database access requires authorization via a separate authentication server, so a theoretical breach to a single customer's account does not jeopardize the data in any other account. This architecture further supports the ability to disable a single customer's account without affecting service for other customers.	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	No	We use industry standard encryption algorithms, such as AES-256. To date we have not had a third party certify FIPS-140 compliance.	
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)	Yes	All session information (including data exchanges between College and SchoolMessenger) is protected by 256-bit SSL encryption certified by Norton Secured, Powered by VeriSign, the trusted industry leader in secure certificate authentication services. They provide the highest level of encryption available to civilians in the US. This means that sensitive information like phone numbers and email addresses is	Summarize your transport encryption strategy.

			fully protected. Moreover, this transport encryption meets the standards for 3DES and AES.	
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	Yes	All data within the application is encrypted at rest using an AES encryption cipher.	Summarize your data encryption strategy.
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	No	We use industry standard encryption algorithms, such as AES-256. To date we have not had a third party certify FIPS-140 compliance.	
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)	Yes	All session information (including data exchanges between College and SchoolMessenger) is protected by 256-bit SSL encryption certified by Norton Secured, Powered by VeriSign. Currently, database connections are not encrypted (for internal system-to-system transmission). All data is encrypted at rest and resides within a private Virtual Private Cloud (VPC) within the Amazon Cloud. In addition, all data resides behind firewalls.	Include all types of encryption; remote-access, application/database, end-user-to-system, etc.

DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	Dispersed throughout the United States. SchoolMessenger is collocated in AWS which has multiple regions, each of which contains multiple zones of availability. As a consequence, our disaster recovery includes failover through multiple regions, as well as failover through the zones of availability.		Ensure that all parts of DATA-07 are clearly stated in your response.
DATA-08	At the completion of this contract, will data be returned to the institution?	Yes	Data can be retrieved from the application interface. Report data would be as CSV files, recordings as mp3 files.	Describe how data will be returned to the institution and in what format will it be presented.
DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?	Yes	Data is retained for up to 12 months by default, in case its of need to the college. However, we can also purge the data immediately at the college's request.	State the length of time that Institution's data will be available in the system at the completion of the contract.
DATA-10	Can the institution extract a full backup of data?	No	As a SaaS deployment, all backups are managed by Intrado.	Summarize why the institution cannot extract a full backup of its data.
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	Yes	All data remains the property of the College.	Provide reference to your data ownership documention.
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes	Intrado will comply with this requirement in full.	Provide references, as needed.
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service,	Yes	Intrado will comply with this requirement in full.	State how the institution will be notified of imminent termination.

	will you provide 90 days for customers to get their data out of the system and migrate applications?			
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	Critical data is replicated in multiple data centers to ensure that information always remains geo-synched. We offer a monitored backup service in which customer data is backed up to disk and securely stored within our facilities. Backup data is tested (restored) every six months to ensure data integrity. Backups are taken on a daily or weekly basis to ensure minimal data loss, and critical data is replicated to multiple datacenter locations. We offer a typical recovery time objective of 15-30 minutes in the event of a catastrophic system failure.		If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.
DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?	Yes	See the above response.	Summarize your backup scheduling strategy.
DATA-16	How long are data backups stored?	Schedules vary based on the nature of the backup.		If your backup strategy uses varying periods, ensure that each strategy is clearly stated and supported.
DATA-17	Are data backups encrypted?	Yes	Yes. All backups are encrypted using an AEA-256 standard and stored in secured storage.	Summarize the encryption algorithm/strategy you are using to secure backups.

DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	Yes	Intrado stores SSL and private keys in a secure vault. For maximum security, only a limited number of authorized staff can access this vault and it requires two-factor authentication.	Summarize your cryptographic key management process.
DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	Yes	Critical data is replicated in multiple data centers to ensure that information always remains geo-synched. We offer a monitored backup service in which customer data is backed up to disk and securely stored within our facilities. Backup data is tested (restored) every six months to ensure data integrity. Backups are taken on a daily or weekly basis to ensure minimal data loss, and critical data is replicated to multiple datacenter locations. We offer a typical recovery time objective of 15-30 minutes in the event of a catastrophic system failure.	Decribe your overall strategy to accomplish these elements.
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)	Yes	Please see our previous response.	Summarize your off site backup strategy.
DATA-21	Are physical backups taken off site? (i.e.	No	Backups reside in our cloud environment. So, technically, they do not leave our siloed instance within the cloud.	State any plans to implement off site

	physically moved off site)			physical backups in your environment.
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	No		
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	Yes	Intrado has detailed policies and procedures for disposing of data and assets, such as computers, hard drives, servers, and other electronic media, all of which align with industry best practices and are crafted in accordance with the above DoD standard. When it comes to customer data, all data of this nature reside on physical hard drives. Any such drives containing customer information that require removal from the production environment are wiped using a procure that complies with the government standard DoD 5220.22M, with certificates being provided upon completion of the data destruction.	Provide details of these procedures (link or attached).
DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	Yes	Yes. Our practice and procedures align with DoD 5220.22-M.	

DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	Yes	Yes. Please see our previous responses for supporting detail.	Provide a general summary of your long-term data retention strategy.
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	Yes	At contract termination, by default, data will be retained for 12 months, in case the information is of need to the college; however, all data will be purged immediately, if so requested. Further, all data is encrypted at rest, stored behind firewalls, and collocated in Tier III data centers.	Provide a general summary of your archival environment.
DATA-27	Will you handle data in a FERPA compliant manner?	Yes	Yes. SchoolMessenger is 100% FERPA compliant and maintains a comprehensive privacy policy. We understand that for you to full advantage of this innovative service, we must ensure your privacy and security, making sure that the privacy and rights of others are also respected. See attachments "SchoolMessenger and FERPA Compliance" immediately following this table.	Describe how FERPA compliance is integrated into your process and procedures.
DATA-28	Is any institution data visible in system administration modules/tools?	Yes	In order to provide notification services to the institution, the institutions data must be available. A significant part of the system administration involves determining the level of access to data for individual end users.	Summarize why the Institution's data is visible in system adminitration modules/tools.
Database		**Vendor Answers**	**Additional Information**	**Guidance**

DBAS-01	Does the database support encryption of specified data elements in storage?	Yes	Yes. All data is encrypted via AEA-256 standard when at rest.	Describe the type of encryption that is supported.
DBAS-02	Do you currently use encryption in your database(s)?	Yes	Yes. All data is encrypted via AEA-256 standard when at rest.	Describe how encryption is leveraged in your database(s).
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	No	The institution's data would reside in our instance of the AWS cloud.	Provide a detailed description of where the Institution's data will reside.
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	The data center is subject to annual SOC 2 Type 2 audits. As AWS does not disclose these reports, we've attached their SOC 3 report immediately following this table.	Obtain the report if possible and add it to your submission.
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	Yes	Yes. Amazon provides 24/7/365 monitoring of their facilities.	Describe the on-site staff capabilities.
DCTR-04	Do any of your servers reside in a co-located data center?	Yes	Yes. We collocate in AWS.	Provide a brief summary of this arrangement.
DCTR-05	Are your servers separated from other companies via a physical barrier, such	Yes	Yes/No. We are separated by a virtual private cloud.	Describe your physical barrier strategy.

	as a cage or hardened walls?			
DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	Yes	Not applicable. We rely on cloud hosting.	Elaborate on your DCTR-05 response, as needed.
DCTR-07	Select the option that best describes the network segment that servers are connected to.	Other		Provide a general summary of the implemented networking strategy.
DCTR-08	Does this data center operate outside of the Institution's Data Zone?	Yes	Yes. However, Intrado selects the data zones and geographic confines for our customers. So, a customer in the United States' data would remain in the United States in our US instance of the application. By contrast, a customer in Canada would be able to have their data siloed within that country in our Canadian instance of SchoolMessenger Communicate.	State the location of the data center and summarize the strategy for this implementation.
DCTR-09	Will any institution data leave the Institution's Data Zone?	No		

DCTR-11	Are your primary and secondary data centers geographically diverse?	Yes	Yes. Our primary and secondary instances are in Oregon and Ohio.	State your primary and secondary data center locations. For cloud infrastructures, state the primary and secondary zones.
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	Yes	With AWS, we have the means to control the data zones and zones of availability that can be used.	Summarize details of the contract, where applicable.
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Tier III		Review the Uptime Institute's level/tier direction provided on their website if you need addition information to answer DCTR-13.
DCTR-14	Is the service hosted in a high availability environment?	Yes	Yes. Please see attachment "Hosting, Security, and Privacy" for additional supporting detail.	Provide a summary to support your response selection.
DCTR-15	Is redundant power available for all datacenters where institution data will reside?	Yes	Yes. Please see attachment "Hosting, Security, and Privacy" for additional supporting detail.	Provide a detailed description of the implemented strategy. (i.e. batteries, generator)

DCTR-16	Are redundant power strategies tested?	Yes	Yes. AWS is subject to regular testing to ensure optimal performance. Please see the attached SOC 3 report for additional supporting detail.	State how often redundant power strategies are tested and the date of the last successful test.
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	AWS, one of the industry leading cloud providers meets or exceeds industry standards for heating, cooling, and fire suppression. Please see the attached SOC 3 Report for supporting detail.		Ensure that all parts of DCTR-17 are clearly stated in your response.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	Please see the attached SOC 3 Report for supporting detail.		State the ISP provider(s) in addition to the number of ISPs that provide connectivity.
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	Yes	We use multiple Tier 1 Voice Telecommunications Networks and delivers messages using best-of-breed VoIP, TDM, SMS, and email technologies. This is another way that we ensure the application has no single point of failure	Provide a brief description for each datacenter.
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**	**Guidance**
DRPL-01	Describe or provide a reference to your	As noted above, we do not disclose full disaster recovery plans without a non-disclosure agreement in		Provide a valid URL to your current DRP or submit it along with

	Disaster Recovery Plan (DRP).	place. Accordingly, many of the supporting details have been left blank.		this fully-populated HECVAT.
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Yes		State the responsible owner, or position title.
DRPL-03	Can the Institution review your DRP and supporting documentation?	Yes		Provide DRP with your submission of this fully-populated HECVAT.
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?	No		
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	Yes		Summarize your disaster recovery strategy including the type of availability your disaster recovery site provides.
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Yes		Summarize your disaster recovery relocation testing strategy.
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Yes		Summarize your problem/issue escalation plan.

DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Yes		Summarize your documented communication plan in your DRP.
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)			Ensure that all elements of DRPL-09 are clearly stated in your response.
DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).	Yes		Provide a summary of the results, including actual recovery time.
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	Yes		Summarize your recovery time capabilities observations.
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes		Summarize your DRP review and update processes and/or procedures.
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service	Yes		Summarize your cyber insurance strategy.

	outages, data that is lost or stolen, and security incidents?			
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**	**Guidance**
FIDP-01	Are you utilizing a web application firewall (WAF)?	Yes	The service uses redundant firewalls from two independent industry-leading manufacturers to provide double the protection and ensure high availability. A security flaw in one firewall layer doesn't compromise the system – or your data. The application uses firewalls with: - Integrated Deep Inspection for application-level attack protection for our Internet facing protocols, applied on a per-policy basis - Denial of service protection to protect against both internal and external attacks. - High-availability capabilities to minimize the potential for a single point of failure - Dynamic routing support to reduce reliance on manual intervention to establish a new route in the event of failure.	Describe the currently implemented WAF.
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	See the above response.	Describe the currently implemented SPI firewall.

FIDP-03	State and describe who has the authority to change firewall rules?	Firewall rules can only be changed by our Technology Service Team after approval by our Information Security Office.		Ensure that all parts of FIDP-03 are clearly stated in your response.
FIDP-04	Do you have a documented policy for firewall change requests?	Yes	All changes are governed by a Formal Change Request Policy.	Describe your documented firewall change request policy.
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	Yes	All systems are monitored 24/7/365. Weekly external vulnerability scans are performed utilizing various off the shelf and homegrown utilities, including Nessus. Monitoring systems are configured to regularly scan for equipment issues or for any indication of issues. Incidents and/or risks are identified and escalated to operations staff 24/7/365.	Describe the currently implemented IDS.
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	Yes	Please see our previous response.	Describe the currently implemented IPS.
FIDP-07	Do you employ host-based intrusion detection?	Yes	Yes. We maintain and monitor security appliances, 24/7/365, to detect abnormal system activity, malware, and viruses. In addition, weekly external vulnerability scans are performed utilizing various off the shelf and homegrown utilities, including Nessus. Monitoring systems are configured to regularly scan for equipment issues or for any indication of issues. Incidents and/or risks are identified and escalated to operations staff 24/7/365.	Describe the currently implemented host-based IDS solution(s).

FIDP-08	Do you employ host-based intrusion prevention?	Yes	See previous response.	Describe the currently implemented host-based IPS solution(s).
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?	No	Yes. We maintain and monitor security appliances, 24/7/365, to detect abnormal system activity, malware, and viruses. In addition, weekly external vulnerability scans are performed utilizing various off the shelf and homegrown utilities, including Nessus. Monitoring systems are configured to regularly scan for equipment issues or for any indication of issues. Incidents and/or risks are identified and escalated to operations staff 24/7/365.	Describe your intent to implement NGPT monitoring.
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	Yes		Provide a brief summary of this activity.
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	Internally and tested using external tools. For instance, at the application level, to identify and eliminate security vulnerabilities, the platform has been subjected to security scans using industry-standard tools such as Nessus. See the response to FIDP-05.		In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Yes		Describe your current network systems logging strategy.

Mobile Applications	**Vendor Answers**	**Additional Information**	**Guidance**

MAPP-01	On which mobile operating systems is your software or service supported?	iOS v9.0+, and Android v4.4+ via Mobile App.		Ensure that all supported operating systems are listed - be sure to provide version number, where relevant.
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	Please see the attached "System Architecture." Please note, the data is not stored on the app.		Ensure that all elements of MAPP-02 are clearly stated in your response. (i.e. (architecture AND functionality are defined)
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?	Yes	SchoolMessenger Admin (Sender App); SchoolMessenger (Recipient App)	State the application title as listed within the trusted source.
MAPP-04	Does the application store, process, or transmit critical data?	Yes	The application is used to send broadcasts, as such, the message content is processed and transmitted through the app. Actual content storage, as well as institution data, stays in the hosted application rather than being passed to the mobile app.	Provide a detailed summary for your response.
MAPP-05	Is Institution's data encrypted in transport?	Yes	All credentials are subject to a salted hash encryption at the point of authentication and are never stored in plain text. Further, all client to server communications are encrypted via SSL 256 bit encryption.	Describe how data is encrypted in transport. (i.e. from system to app)

MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)	Yes	Yes. See the above response. Please note, institution data is not stored on the device itself.	Describe how data is encrypted in storage. (i.e. at-rest within the app)
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?	Yes	The system supports authentication via LDAP and SAML, as well as direct log in access.	Summarize your system authentication capabilities.
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	Yes	The system supports authentication via LDAP and SAML, as well as direct log in access. The college will determine if one of these systems is appropriate or required.	Summarize any requirements for the Institution to take advantage of these capabilities.
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?	Yes		Summarize your secure coding practices.
MAPP-10	Has the application been tested for vulnerabilities by a third party?	Yes	We provide extensive internal testing and the platform is subject to industry standard tools such as Nessus.	State the party that performed the test and the date it was conducted. Provide test results and mitigation plans, if any.
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?			Ensure that all elements of MAPP-11 are clearly stated in your response.

Physical Security	**Vendor Answers**	**Additional Information**	**Guidance**

PHYS-01	Does your organization have physical security controls and policies in place?	Yes	All Intrado offices are subject to video surveillance.	Provide a copy of your physical security controls and policies along with this document (link or attached).
PHYS-02	Are employees allowed to take home Institution's data in any form?	No	Sensitive client information is never stored on non-company owned assets. Further, as noted above, access to your data is limited to essential personnel. Those select individuals have the means to access the data via a combination of encrypted VPN, machine certificates, and authentication (via unique user names and passwords). This combination is utilized to safeguard any remote sessions. And, all access is fully tracked and auditable to further maximize security.	
PHYS-03	Are video monitoring feeds retained?	Yes		State the retention period for security video.
PHYS-04	Are video feeds monitored by datacenter staff?	Yes		Summarize your video monitoring strategy for datacenter staff.
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	Yes		Summarize your process and procedure for the installation and removal of equipment to/from your environment.

Policies, Procedures, and Processes		Vendor Answers	Additional Information	Guidance
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Yes	At a high-level, we've attached a summary document titled "Hosting, Security, and Privacy". We have a full-time information security team and maintain hundreds of pages of information security policies and procedures.	Provide a links to these documents in Additional Information or attach them with your submission. Include the responsible party for your information security program and the size of your security staff.
PPPR-02	Do you have a documented patch management process?	Yes	Yes. The platform is constantly monitored for vulnerabilities and patches are evaluated within 30 days of release. However, deployment schedules vary based on testing and our ability to confirm stability prior to deployment. Where possible, patches and software updates are performed during our standard maintenance window. When patches and updates are deemed essential, emergency maintenance is ordered, and it occurs outside of standard business hours.	Summarize your documented patch management process.
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes	We'd need additional details regarding the specific type of standard to fully confirm compliance.	Summarize any limitations to your accomodation capabilities.

PPPR-04	Have your developers been trained in secure coding techniques?	Yes	Intrado follows standard SSDLC phases including planning, design, testing, implementation, and ongoing maintenance. Security QA begins with a process of rigorous code reviews to identify any potential security flaws. Application components are then thoroughly tested through a series of manual and automated tests cases designed to test the authentication, validation, restriction, and logging features. Any issues encountered in testing are logged and corrective measures are taken. Tests are repeated and no code goes into production until all identifiable issues have been resolved. Web code reviews are performed as a regular part of the security QA process and the quarterly security audits.	Provide a brief description of the training provided.
PPPR-05	Was your application developed using secure coding techniques?	Yes	Yes. See our previous response for supporting details.	Describe the secure coding techniques used to develop your application.
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?	Yes	Yes. See our previous response to PPPR-04.	Provide a list of all tools utilized during static code analysis or static application security testing.

PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?	Yes	Yes. See our previous response to PPPR-04.	Describe testing processes, including but not limited to, development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results.
PPPR-08	Are information security principles designed into the product lifecycle?	Yes	Yes. See our previous response to PPPR-04.	Summarize the information security principles designed into the product lifecycle.
PPPR-09	Do you have a documented systems development life cycle (SDLC)?	Yes	Yes. See our previous response to PPPR-04.	Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).
PPPR-10	Do you have a formal incident response plan?	Yes	Disclosure of the plan and procedures would require a non-disclosure agreement.	Summarize your formal incident response plan.

PPPR-11	Will you comply with applicable breach notification laws?	Yes	Yes. We will comply with applicable breach notification laws.	State how quickly the Institution will be notified of a data breach or security incident.
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	Yes		State that you have reviewed the Institution's IT policies with regards to user privacy and data protection.
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?	Yes		
PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	Yes	We maintain a comprehensive hiring, training, and retraining process, which includes rigorous pre-employment screening (including full criminal background checks); • Additionally, each employee, as part of the hiring process, signs agreements and statements including but not limited to: o Non-disclosure agreement; o Confidentiality agreement; and, o Company policy acknowledgement and agreement.	Summarize your background check practices.
PPPR-15	Do you require new employees to fill out agreements and review policies?	Yes	Yes. See the previous response.	Summarize the required agreements and reviewed policies.

PPPR-16	Do you have documented information security policy?	Yes	We have full bodies of literature documenting our security policies.	Provide a reference to your information security policy or submit documentation with this fully-populated HECVAT.
PPPR-17	Do you have an information security awareness program?	Yes	Yes. We have a team of over 65 full-time employees who are solely focused on information security. This includes a focus on policies, procedures, and training. And, each employee is subject to	Summarize your information security awareness program.
PPPR-18	Is security awareness training mandatory for all employees?	Yes		Summarize your security awareness training content and state how frequently employees are required to undergo security awareness training.
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	Yes		Provide a brief summary and the implement review interval.
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?	Yes		Summarize your internal audit processes and procedures.

Product Evaluation		Vendor Answers	Additional Information	Guidance
PROD-01	Do you incorporate customer feedback into security feature requests?	Yes		Provide a reference to your customer feedback procedures.
PROD-02	Can you provide an evaluation site to the institution for testing?	Yes		Summarize the scope of your evaluation site(s) and request procedures. Provide references, as needed.
Quality Assurance		**Vendor Answers**	**Additional Information**	**Guidance**
QLAS-01	Provide a general summary of your Quality Assurance program.	Security Quality Assurance (QA) begins with a process of rigorous code reviews to identify any potential security flaws. Application components are then thoroughly tested through a series of manual and automated tests cases designed to test the authentication, validation, restriction, and logging features. Any issues encountered in testing are logged and corrective measures are taken. Tests are repeated and no code goes into production until all identifiable issues have been resolved. Web code reviews are performed as a regular part of the security QA process. Further, the application is subject to Nessus testing.		Provide a valid URL to your Quality Assurance program or submit it along with this fully-populated HECVAT.
QLAS-02	Do you comply with ISO 9001?	Yes	AWS is subject to an annual ISO 90001 audit. See the attached SOC 3 Report for additional details.	If certified, provide supporting documentation.

QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	Yes	Yes. We can easily provide this information under a non-disclosure agreement.	Provide references to quality and performance metrics documentation.
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	Yes	Yes. SCCC has trusted our products and services since 2014.	Provide the Institution's contact, describe the products and/or services offered, and the total value of the services provided.
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	Yes	We have regular webinars on trends and issues that could impact our clients. This includes FCC changes, TCPA rulings, and many other topics.	Summarize your informational program.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**
SYST-01	Are systems that support this service managed via a separate management network?	Yes	Yes. The SchoolMessenger application is separate from the Intrado servers and network.	Summarize how this is implemented in your environment.
SYST-02	Do you have an implemented system configuration management process?	Yes		Summarize your implemented system configuration management precess.

	(e.g. secure "gold" images, etc.)			
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	Yes	Yes. All employees are subject to annual MDM training and Intrado can perform a remote wipe on any phone if it believes security has been compromised.	Summarize your on-site MDM capabilities.
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	Yes	Yes. We have full policies, procedures, and annual retraining on all of these areas.	Summarize your systems management and configuration strategy.
Vulnerability Scanning		**Vendor Answers**	**Additional Information**	**Guidance**
VULN-01	Are your *applications* scanned externally for vulnerabilities?	Yes		Decribe your external application vulnerability scanning strategy.
VULN-02	Have your applications had an external vulnerability assessment in the last year?	No	Maybe yes - it depends on how we see "external"	Describe any plans to have application external assessment(s) performed on your systems.

VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	Yes	The platform is constantly monitored for vulnerabilities. Patches are evaluated within 30 days of release. However, deployment schedules vary based on testing and our ability to confirm stability prior to deployment.	Summarize your vulnerability scanning strategy.
VULN-04	Are your *systems* scanned externally for vulnerabilities?	Yes		Decribe your external system vulnerability scanning strategy.
VULN-05	Have your systems had an external vulnerability assessment in the last year?	Yes		State the date of your most recent system external assessment.
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	We employ a wide range of performance monitoring tools to ensure the integrity and availability of our services. Examples include, but are not limited to New Relic, Thousand Eyes, Keynote, and Google Analytics. In addition, Weekly external vulnerability scans are performed utilizing various off the shelf and homegrown utilities, including Nessus. Monitoring systems are configured to regularly scan for equipment issues or for any indication of issues. Incidents and/or risks are identified and escalated to operations staff 24/7/365.		Ensure that all elements of VULN-06 are clearly stated in your response.
VULN-07	Will you provide results of security scans to the Institution?	Yes	We are open to discussing disclosure of results. We'd need additional detail in order to determine if such a disclosure could be made under a non-disclosure agreement.	Provide a reference to security scan documentation.

VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	See our earlier response to VULN-06.		Ensure that all elements of VULN-08 are clearly stated in your response.
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	Yes	We are open to discussing the testing needs with the College. Ultimately, as the platform relies on a shared server configuration, we'd need additional details to confirm if and how such	Provide reference to the process or procedure to setup security testing times and scopes.
HIPAA - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	No	As a corporation, we comply with most of the following requirements, as we provide a wide range of products and services, including those specialized for the healthcare arena. As these questions and answers are focused exclusively on the solution proposed in this RFP response, SchoolMessenger Communicate, this entire section is not application as the platform neither uses nor stores private health information.	Refer to HIPAA regulations documentation for supplemental guidance in this section.

HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.

	Have you identified areas of risks?	No		Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Have you taken actions to mitigate the identified risks?	No		Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.

HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-16	Does your application provide the ability to define user access levels?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-18	Does your application support varying levels of access to records based on user ID?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-19	Is there a limit to the number of groups a user can be assigned?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.

HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-23	How long does the application keep access/change logs?	N/A		Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-24	Can the application logs be archived?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.

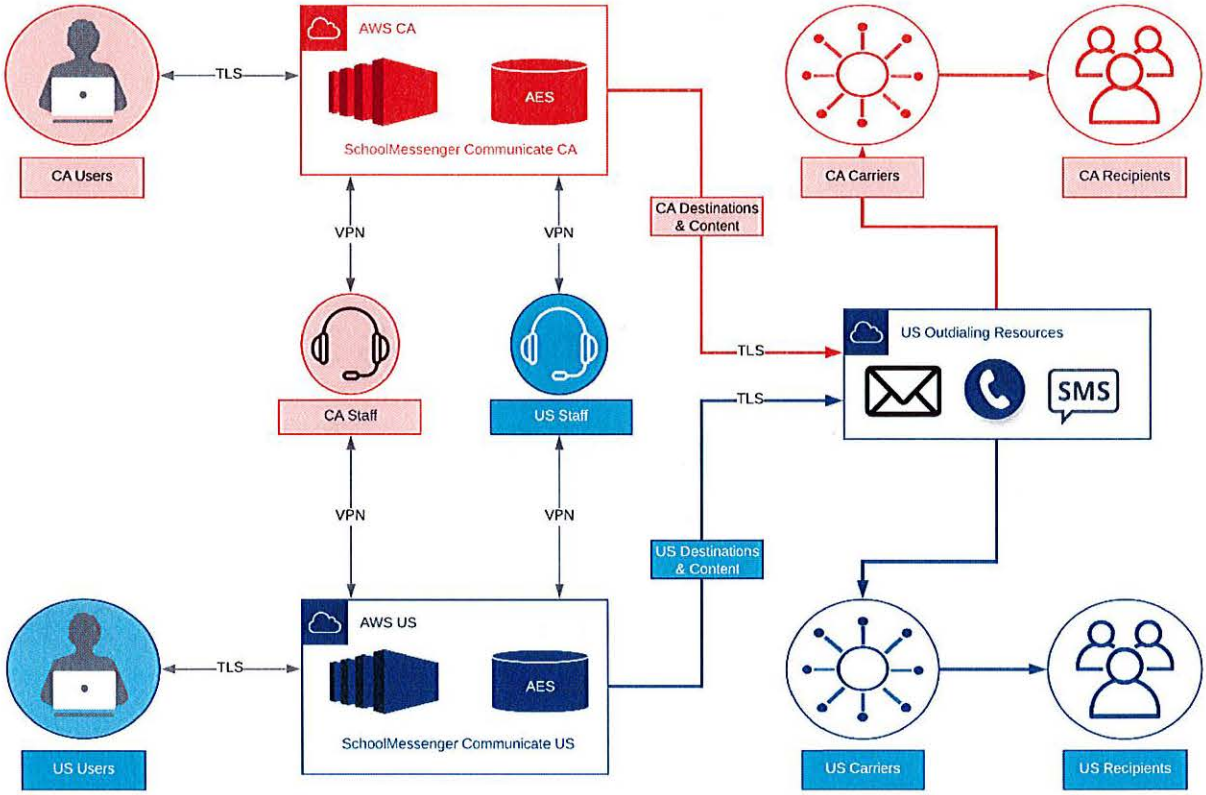
	Can the application logs be saved externally?			
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?	No		Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Have the policies/plans mentioned above been tested?			
	Can you provide a HIPAA compliance attestation document?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Are you willing to enter into a Business Associate Agreement (BAA)?	No	N/A	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Have you entered into a BAA with all subcontractors who may have access to	No	N/A	Refer to HIPAA regulations documentation for

	protected health information (PHI)?			supplemental guidance in this section.
PCI DSS - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	No	Not applicable. The system does not process or store credit cards or any other data governed by PCI DSS.	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-04	Are you classified as a service provider?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-05	Are you on the list of VISA approved service providers?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section

PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	N/A		Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-08	What payment processors/gateways does the system support?	N/A		Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-10	Is the application listed as an approved PA-DSS application?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	No	N/A	Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features	N/A		Refer to PCI DSS Security Standards for supplemental guidance in this section

	or capabilities of the system that must be added or changed in order to operate in compliance with the standards.		

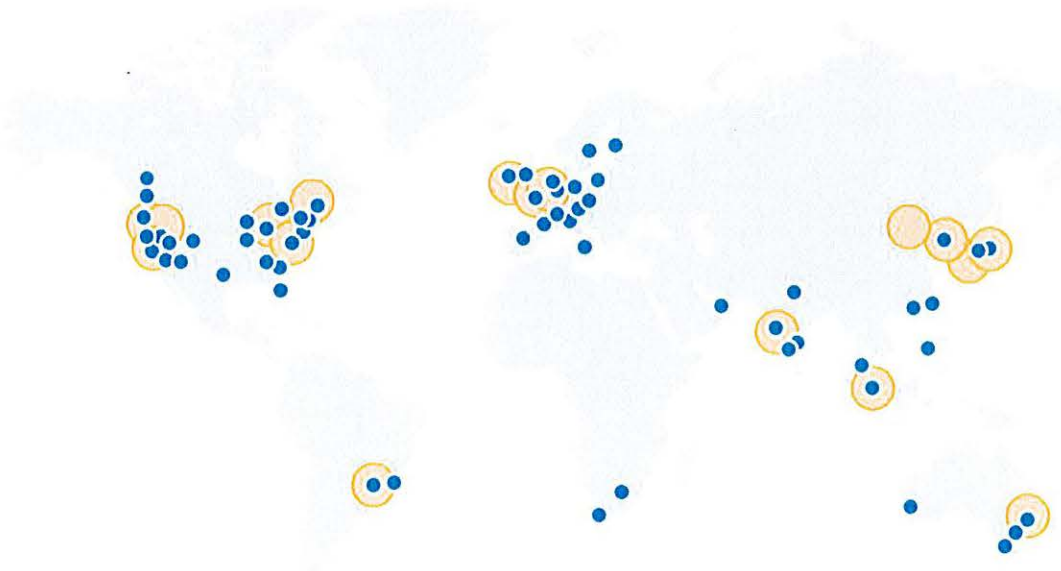
SYSTEM ARCHITECTURE



System and Organization Controls 3 (SOC 3) Report

Report on the Amazon Web Services System Relevant to Security, Availability, and Confidentiality

For the Period October 1, 2018 – March 31, 2019



Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Amazon Web Services, Inc.

Scope:

We have examined management's assertion, contained within the accompanying "Report on the Amazon Web Services System Relevant to Security, Availability, and Confidentiality" (Assertion), that Amazon Web Services, Inc.'s (AWS) controls over the Amazon Web Services System (System) were effective throughout the period October 1, 2018 to March 31, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Management's Responsibilities

AWS' management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Amazon Web Services System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the Amazon Web Services System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of AWS' relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating AWS' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Building a better working world

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve AWS' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, AWS' management's assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

Ernst & Young LLP

April 26, 2019

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

Management's Report of its Assertions on the Effectiveness of Its Controls Over the Amazon Web Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of, Amazon Web Services, Inc. are responsible for

- Identifying the AWS Web Services System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period October 1, 2018 to March 31, 2019 to provide reasonable assurance that the principle service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.*

Very truly yours,

Amazon Web Services Management

AWS Background

Since 2006, Amazon Web Services (AWS) has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. With AWS, customers can deploy solutions on a cloud computing environment that provides compute power, storage, and other application services over the Internet as their business needs demand. AWS affords businesses the flexibility to employ the operating systems, application programs, and databases of their choice.

The scope covered in this report consists of the following services (the service name is followed by the services's namespace[1] in parenthesis):

- AWS Amplify Console (amplify)
- API Gateway (apigateway)
- AWS AppSync (appsync)
- Amazon Athena (athena)
- AWS Auto Scaling (autoscaling)
- AWS Backup (backup)
- AWS Batch (batch)
- AWS Certificate Manager (acm)
- Amazon Cloud Directory (clouddirectory)
- AWS CloudFormation (cloudformation)
- Amazon CloudFront (cloudfront)
- AWS CloudHSM (cloudhsm)
- AWS CloudTrail (cloudtrail)
- Amazon CloudWatch (cloudwatch, events,logs)
- AWS CodeBuild (codebuild)
- AWS CodeCommit (codecommit)
- AWS CodeDeploy (codedeploy)
- Amazon Cognito (cognito-idp, cognito-identity, cognito-sync)
- Amazon Comprehend (comprehend)
- AWS Config (config)
- Amazon Connect (connect)
- AWS Database Migration Service (dms)
- AWS DataSync (datasync)
- AWS Direct Connect (directconnect)
- AWS Directory Service (ds) – [Excludes Simple Active Directory]
- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB (dynamodb)
- AWS IoT Device Management (iot)
- AWS IoT Greengrass (greengrass)
- AWS Key Management Service (kms)
- Amazon Kinesis Data Analytics (kinesisanalytics)
- Amazon Kinesis Data Firehose (firehose)
- Amazon Kinesis Data Streams (kinesis)
- Amazon Kinesis Video Streams (kinesisvideo)
- AWS Lambda (lambda)
- Amazon Macie (macie)
- AWS Managed Services
- Amazon MQ (mq)
- Amazon Neptune (neptune-db)
- AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (opsworks-cm)
- AWS OpsWorks (opsworks)
- AWS Organizations (organizations)
- Amazon Pinpoint (mobiletargeting)
- Amazon Polly (polly)
- Amazon QuickSight (quicksight)
- Amazon Redshift (redshift)
- Amazon Rekognition (rekognition)
- Amazon Relational Database Service (rds)
- AWS Resource Groups (resource-groups)
- AWS RoboMaker (robomaker)
- Amazon Route 53 (route53)
- Amazon SageMaker (sagemaker)
- AWS Secrets Manager (secretsmanager)
- AWS Security Hub (security)

[1] When customers create IAM policies or work with Amazon Resource Names (ARNs), customers identify an AWS service using a *namespace*. For example, the namespace for Amazon S3 is s3, and the namespace for Amazon EC2 is ec2. Customers use namespaces when identifying actions and resources across AWS.

- AWS Elastic Beanstalk (elasticbeanstalk)
- Amazon Elastic Block Store (ec2)
- Amazon Elastic Compute Cloud (ec2)
- Amazon Elastic Container Registry (ecr)
- Amazon Elastic Container Service (ecs) – [both Fargate and EC2 launch types]
- Amazon Elastic Container Service for Kubernetes (eks)
- Amazon Elastic File System (elasticfilesystem)
- Amazon Elasticsearch Service (es)
- Elastic Load Balancing (elasticloadbalancing)
- Amazon ElastiCache (elasticache)
- AWS Elemental MediaConnect (mediaconnect)
- Amazon EMR (elasticmapreduce)
- AWS Firewall Manager (fms)
- Amazon FreeRTOS (signer)
- Amazon FSx (fsx)
- Amazon Glacier (glacier)
- AWS Global Accelerator (globalaccelerator)
- AWS Glue (glue)
- AWS GuardDuty (guardduty)
- AWS Identity and Access Management (iam)
- VM Import/Export
- Amazon Inspector (inspector)
- AWS IoT Core (iot)
- AWS Server Migration Service (sms)
- AWS Serverless Application Repository (serverlessrepo)
- AWS Service Catalog (servicecatalog)
- AWS Shield (shield, DDoSProtection)
- Amazon Simple Email Service (ses)
- Amazon Simple Notification Service (sns)
- Amazon Simple Queue Service (sqs)
- Amazon Simple Storage Service (s3)
- Amazon Simple Workflow Service (swf)
- Amazon SimpleDB (sdb)
- AWS Snowball (snowball)
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions (states)
- AWS Storage Gateway (storagegateway)
- AWS Systems Manager (ssm)
- AWS Transfer for SFTP (transfer)
- Amazon Translate (translate)
- Amazon Virtual Private Cloud (Amazon VPC) (ec2)
- AWS WAF (waf)
- Amazon WorkDocs (workdocs)
- Amazon WorkLink (worklink)
- Amazon WorkMail (workmail)
- Amazon WorkSpaces (workspaces)
- AWS X-ray (xray)

The scope of locations covered in this report includes the data centers in the US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), GovCloud (US West), GovCloud (US East), Canada (Montreal), Europe (Ireland), Europe (Frankfurt), Europe (London), Europe (Paris), Europe (Stockholm), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Asia Pacific (Osaka)[2], Asia Pacific (Seoul), Asia Pacific (Mumbai), and South America (São Paulo) Regions. The following AWS Edge locations are also covered in this report:

- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Sydney, Australia
- Vienna, Austria
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Montréal, Canada
- Chennai, India
- Hyderabad, India
- Mumbai, India
- New Delhi, India
- Dublin, Ireland
- Milan, Italy
- Palermo, Italy
- Osaka, Japan
- Dubai, United Arab Emirates
- Fujairah, United Arab Emirates
- Arizona, United States
- California, United States
- Colorado, United States
- Florida, United States
- Georgia, United States
- Illinois, United States

[2] The Asia Pacific (Osaka) Local Region is a Local Region, which comprises an isolated, fault-tolerant infrastructure design consisting of three virtual Availability Zones located in the same data center and is intended to be used in conjunction with the Asia Pacific (Tokyo) Region. This region requires that customers request access through a sales representative.

- Toronto, Canada
- Vancouver, Canada
- Prague, Czech Republic
- Hong Kong, China
- Copenhagen, Denmark
- London, England
- Manchester, England
- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Munich, Germany
- Bengaluru, India
- Tokyo, Japan
- Seoul, Korea
- Kuala Lumpur, Malaysia
- Amsterdam, Netherlands
- Oslo, Norway
- Manila, Philippines
- Warsaw, Poland
- Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- Taipei, Taiwan
- Indiana, United States
- Massachusetts, United States
- Minnesota, United States
- Nevada, United States
- New Jersey, United States
- New York, United States
- Ohio, United States
- Oregon, United States
- Pennsylvania, United States
- Texas, United States
- Virginia, United States
- Washington, United States

Infrastructure

AWS operates the cloud infrastructure that customers may use to provision computing resources such as processing and storage. The AWS infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. The AWS infrastructure is designed and managed in accordance with security compliance standards and AWS best practices.

Components of the System

AWS offers a series of Analytics; Application Integration; Business Productivity; Compute; Customer Engagement; Database; Desktop & App Streaming; Developer Tools; Internet of Things; Management Tools; Media Services; Migration; Mobile Services; Network & Content Delivery; Security, Identity, and Compliance; and Storage services. A description of the AWS services included within the scope of this report is listed below:

AWS Amplify Console (amplify)

AWS Amplify makes it easy to create, configure, and implement scalable mobile and web apps powered by AWS. Amplify seamlessly provisions and manages the mobile backend and provides a simple framework to easily integrate the backend with the iOS, Android, Web, and React Native frontends. Amplify also automates the application release process of both the frontend and backend allowing the customers to deliver features faster.

API Gateway (apigateway)

API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With Amazon API Gateway, customers can create a custom API to code running in AWS Lambda, and then call the Lambda code from customers' API.

AWS AppSync (appsync)

AWS AppSync automatically updates the data in web and mobile applications in real time, and updates data for offline users as soon as they reconnect. AWS AppSync makes it easy to build collaborative mobile and web applications that deliver responsive, collaborative user experiences.

Amazon Athena (athena)

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure for customers to manage. Athena is highly available; and executes queries using compute resources across multiple facilities and multiple devices in each facility. Amazon Athena uses Amazon S3 as its underlying data store, making customers' data highly available and durable.

AWS Auto Scaling (autoscaling)

Auto Scaling launches/terminates instances on a customer's behalf according to conditions customers define, such as schedule, changing metrics like average CPU utilization, or health of the instance as determined by EC2 or ELB health checks. It allows customers to have balanced compute across multiple availability zones and scale their fleet based on usage.

AWS Backup (backup)

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway.

AWS Batch (batch)

AWS Batch enables developers, scientists, and engineers to run batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. AWS Batch plans, schedules, and executes customers' batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances.

AWS Certificate Manager (acm)

AWS Certificate Manager is a service that lets the customer provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and their internal connected resources.

Amazon Cloud Directory (clouddirectory)

Amazon Cloud Directory enables customers to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions. Customers also can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries.

AWS CloudFormation (cloudformation)

AWS CloudFormation enables customers to create and manage a collection of related AWS resources by providing templates to use in the provisioning and updating of AWS services.

Amazon CloudFront (cloudfront)

Amazon CloudFront is a web service that speeds up distribution of customers' static and dynamic web content. CloudFront delivers customers' content through a worldwide network of Edge locations.

AWS CloudHSM (cloudhsm)

AWS CloudHSM is a service that allows customers to use dedicated hardware security module (HSM) appliances within the AWS cloud. AWS CloudHSM allows customers to store and use encryption keys within HSM appliances in AWS data centers.

AWS CloudTrail (cloudtrail)

AWS CloudTrail is a web service that records AWS activity for customers and delivers log files to a specified Amazon S3 bucket. AWS CloudTrail provides a history of AWS API calls for customer accounts.

Amazon CloudWatch (cloudwatch, events, logs)

Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides the customers with data and actionable insights to monitor their applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

AWS CodeBuild (codebuild)

AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild scales continuously and processes multiple builds concurrently, so that customers' builds are not left waiting in a queue. Customers can use prepackaged build environments or can create custom build environments that use their own build tools. AWS CodeBuild eliminates the need to set up, patch, update, and manage customers' build servers and software.

AWS CodeCommit (codecommit)

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It allows teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need for customers to operate their own source control system or worry about scaling their infrastructure.

AWS CodeDeploy (codedeploy)

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and the customer's on-premises servers.

Amazon Cognito (cognito-idp, cognito-identity, cognito-sync)

Amazon Cognito lets customers add user sign-up, sign-in, and manage permissions for mobile and web applications. Customers can create their own user directory within Amazon Cognito. Customers can also choose to authenticate users through social identity providers such as Facebook, Twitter, or Amazon; with SAML identity solutions; or by using customers' own identity system.

Amazon Comprehend (comprehend)

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. Amazon Comprehend uses machine learning to help the customers uncover the insights and relationships in their unstructured data.

AWS Config (config)

AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows customers to automate the evaluation of recorded configurations against desired configurations.

Amazon Connect (connect)

Amazon Connect is a self-service, cloud-based contact center service that enables dynamic, personal, and natural customer engagement at any scale. The self-service graphical interface allows the customers to design contact flows, manage agents, and track performance metrics.

AWS Database Migration Service (dms)

AWS Database Migration Service enables customers to migrate databases between similar and different database programs in the cloud and off-cloud. The service supports homogenous migrations within one database platform, as well as heterogeneous migrations between different database platforms.

AWS DataSync (datasync)

AWS DataSync is a data transfer service that makes it easy for customers to automate moving data between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync automatically handles many of the tasks related to data transfers that can slow down migrations or burden customers' IT operations, including running customers own instances, handling encryption, managing scripts, network optimization, and data integrity validation.

AWS Direct Connect (directconnect)

AWS Direct Connect enables customers to establish a dedicated network connection between their network and one of the AWS Direct Connect locations. Using AWS Direct Connect, customers can establish private connectivity between AWS and their datacenter, office, or colocation environment.

AWS Directory Service (ds) – [Excludes Simple Active Directory]

AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, enables customers' directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Microsoft AD stores directory content in encrypted Amazon Elastic Block Store volumes using encryption keys that AWS manages.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. Amazon DocumentDB is designed from the ground-up to give customers the performance, scalability, and availability customers need when operating mission-critical MongoDB workloads at scale.

Amazon DynamoDB (dynamodb)

Amazon DynamoDB is a managed NoSQL database service. Amazon DynamoDB enables customers to offload to AWS the administrative burdens of operating and scaling distributed databases such as hardware provisioning, setup and configuration, replication, software patching, and cluster scaling.

AWS Elastic Beanstalk (elasticbeanstalk)

AWS Elastic Beanstalk is an application container launch program for customers to launch and scale their applications on top of AWS. Customers can use AWS Elastic Beanstalk to create new environments using Elastic Beanstalk curated programs and their applications, deploy application versions, update application configurations, rebuild environments, update AWS configurations, monitor environment health and availability, and build on top of the scalable infrastructure.

Amazon Elastic Block Store (ec2)

Amazon Elastic Block Store provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Storage volumes behave like raw, unformatted block devices, with user supplied device names and a block device interface. Customers can create a file system on top of Amazon EBS volumes, or use them in any other way one would use a block device (like a hard drive).

Amazon Elastic Compute Cloud (ec2)

Amazon Elastic Compute Cloud is Amazon's Infrastructure as a Service (IaaS) offering, which provides scalable computing capacity using server instances in AWS' data centers. Amazon EC2 is designed to make web-scale computing easier by enabling customers to obtain and configure capacity with minimal friction. Customers create and launch instances, which are virtual machines that are available in a wide variety of hardware and software configurations.

Amazon Elastic Container Registry (ecr)

Amazon Elastic Container Registry is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon Elastic Container Registry is integrated with Amazon Elastic Container Service.

Amazon Elastic Container Service (ecs) – [both Fargate and EC2 launch types]

Amazon Elastic Container Service is a highly scalable, high performance container management service that supports Docker containers and allows customers to easily run applications on a managed cluster of Amazon EC2 instances. Amazon Elastic Container Service eliminates the need for customers to install, operate, and scale customers' own cluster management infrastructure.

Amazon Elastic Container Service for Kubernetes (eks)

Amazon Elastic Container Service for Kubernetes (Amazon EKS) makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS. Amazon EKS runs the Kubernetes management infrastructure for the customer across multiple AWS availability zones to eliminate a single point of failure.

Amazon Elastic File System (elasticfilesystem)

Amazon Elastic File System provides file storage for Amazon EC2 instances that grows and shrinks elastically as data is added and deleted by users. Amazon EFS spreads data across multiple Availability Zones; in the event that an Availability Zone is not reachable, the structure allows customers to still access their full set of data.

Amazon Elasticsearch Service (es)

Amazon Elasticsearch Service is a fully managed service that makes it easy for the customer to deploy, secure, and operate Elasticsearch at scale with zero down time. Amazon Elasticsearch Service lets the customers pay only for what they use – there are no upfront costs or usage requirements.

Elastic Load Balancing (elasticloadbalancing)

Elastic Load Balancing provides customers with a load balancer that automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It allows customers to achieve greater levels of fault tolerance for their applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.

Amazon ElastiCache (elasticache)

Amazon ElastiCache automates management tasks for in-memory cache environments, such as patch management, failure detection, and recovery. It works in conjunction with other AWS services to provide a managed in-memory cache.

AWS Elemental MediaConnect (mediaconnect)

AWS Elemental MediaConnect is a high-quality transport service for live video. MediaConnect enables customers to build mission-critical live video workflows in a fraction of the time and cost of satellite or fiber services.

Amazon EMR (elasticmapreduce)

Amazon EMR is a web service that provides managed Hadoop clusters on Amazon EC2 instances running a Linux operating system. Amazon EMR actively manages clusters for customers, replacing failed nodes and adjusting capacity as requested.

AWS Firewall Manager (fms)

AWS Firewall Manager is a security management service that makes it easier to centrally configure and manage AWS WAF rules across customer accounts and applications. Using Firewall Manager, customers can roll out AWS WAF rules for their Application Load Balancers and Amazon CloudFront distributions across accounts in AWS Organizations.

Amazon FreeRTOS (signer)

Amazon FreeRTOS is an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage.

Amazon FSx (fsx)

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides the customers with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA).

Amazon Glacier (glacier)

Amazon Glacier is an archival storage solution for data that is infrequently accessed for which retrieval times of several hours are suitable. Amazon Glacier enables customers to set access policies on their vaults for users within their AWS Account.

AWS Global Accelerator (globalaccelerator)

AWS Global Accelerator is a networking service that improves the availability and performance of the applications that customers offer to their global users. AWS Global Accelerator is easy to set up, configure and manage.

AWS Glue (glue)

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. The customers can create and run an ETL job with a few clicks in the AWS Management Console.

AWS GuardDuty (guardduty)

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect the customers' AWS accounts and workloads. With GuardDuty, the customers now have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud.

AWS Identity and Access Management (iam)

AWS Identity and Access Management is a web service that helps customers securely control access to AWS resources for their users. Customers use IAM to control who can use their AWS resources (authentication) and what resources they can use and in what ways (authorization).

VM Import/Export

AWS Import/Export is a service that enables customers to import virtual machine images from their existing environment to Amazon EC2 instances and export them back to their off-cloud environment.

Amazon Inspector (inspector)

Amazon Inspector is an automated security assessment service for customers seeking to improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

AWS IoT Core (iot)

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core provides secure communication and data processing across different kinds of connected devices and locations so that customers can easily build IoT applications such as industrial solutions and connected home solutions.

AWS IoT Device Management (iot)

AWS IoT Device Management provides customers with ability to securely onboard, organize, and remotely manage IoT devices at scale. With AWS IoT Device Management, customer can register their connected devices individually or in bulk, and manage permissions so that devices remain secure.

AWS IoT Greengrass (greengrass)

AWS IoT Greengrass seamlessly extends AWS to edge devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage.

AWS Key Management Service (kms)

AWS Key Management Service allows users to create and manage cryptographic keys. One class of keys, Customer Master Keys (CMKs), are designed to never be exposed in plaintext outside the service. CMKs can be used to encrypt data directly submitted to the service. CMKs can also be used to protect other types of keys, Data Encryption Keys (DEKs), which are created by the service and returned to the user's application for local use. AWS KMS only creates and returns DEKs to users; the service does not store or manage DEKs.

Amazon Kinesis Data Analytics (kinesisanalytics)

Amazon Kinesis Data Analytics is the easiest way for customers to analyze streaming data, gain actionable insights, and respond to business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services.

Amazon Kinesis Data Firehose (firehose)

Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards customers are already using today.

Amazon Kinesis Data Streams (kinesis)

Amazon Kinesis Streams is a platform for streaming data on AWS, so customers can load and analyze streaming data. Amazon Kinesis Streams also provides the ability to build custom streaming data applications for specialized needs.

Amazon Kinesis Video Streams (kinesisvideo)

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales the infrastructure needed to ingest streaming video data from millions of devices.

AWS Lambda (lambda)

AWS Lambda lets customers run code without provisioning or managing servers on their own. AWS Lambda uses a compute fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones in a region, which provides the high availability, security, performance, and scalability of the AWS infrastructure.

Amazon Macie (macie)

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides customers with dashboards and alerts that give visibility into how this data is being accessed or moved.

AWS Managed Services

AWS Managed Services provides ongoing management of a customer's AWS infrastructure. AWS Managed Services automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support a customer's infrastructure.

Amazon MQ (mq)

Amazon MQ is a managed message broker service for Apache ActiveMQ that sets up and operates message brokers in the cloud. Message brokers allow different software systems – often using different programming languages, and on different platforms – to communicate and exchange information. Amazon MQ manages the administration and maintenance of ActiveMQ, a popular open-source message broker.

Amazon Neptune (neptune-db)

Amazon Neptune is a fast, reliable, fully managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency.

AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (opsworks-cm)

AWS OpsWorks for Chef Automate is a fully managed configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks also maintains customers' Chef server by automatically patching, updating, and backing up customers' server.

AWS OpsWorks (opsworks)

AWS OpsWorks Stacks is an application and server management service. OpsWorks Stacks lets customers manage applications and servers on AWS and on-premises. With OpsWorks Stacks, customers can model their application as a stack containing different layers, such as load balancing, database, and application server. They can deploy and configure Amazon EC2 instances in each layer or connect other resources such as Amazon RDS databases.

AWS Organizations (organizations)

AWS Organizations helps customers centrally govern their environment as customers' grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps customers to centrally manage billing; control access, compliance, and security; and share resources across customer AWS accounts.

Amazon Pinpoint (mobiletargeting)

Amazon Pinpoint helps customers engage with their customers by sending email, SMS, and mobile push messages. The customers can use Amazon Pinpoint to send targeted messages (such as promotional alerts and customer retention campaigns), as well as direct messages (such as order confirmations and password reset messages) to their customers.

Amazon Polly (polly)

Amazon Polly is a service that turns text into lifelike speech, allowing customers to create applications that talk, and build entirely new categories of speech-enabled products. Amazon Polly is a Text-to-Speech service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice.

Amazon QuickSight (quicksight)

Amazon QuickSight is a fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from customers' data. Using this cloud-based service customers can connect to their data, perform advanced analysis, and create visualizations and dashboards that can be accessed from any browser or mobile device.

Amazon Redshift (redshift)

Amazon Redshift is a data warehouse service to analyze data using a customer's existing Business Intelligence (BI) tools. Amazon Redshift also includes Redshift Spectrum, allowing customers to directly run SQL queries against Exabytes of unstructured data in Amazon S3.

Amazon Rekognition (rekognition)

The easy-to-use Rekognition API allows customers to automatically identify objects, people, text, scenes, and activities, as well as detect any inappropriate content. Developers can quickly build a searchable content library to optimize media workflows, enrich recommendation engines by extracting text in images, or integrate secondary authentication into existing applications to enhance end-user security.

Amazon Relational Database Service (rds)

Amazon Relational Database Service enables customers to set up, operate, and scale a relational database in the cloud. Amazon RDS manages backups, software patching, automatic failure detection, and recovery. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

AWS Resource Groups (resource-groups)

AWS Resource Groups is service that helps customers organize AWS resources into logical groupings. These groups can represent an application, a software component, or an environment.

AWS RoboMaker (robomaker)

AWS RoboMaker is a service that makes_it easy to develop, test, and deploy intelligent robotics applications at scale. RoboMaker extends the most widely used open-source robotics software framework, Robot Operating System (ROS), with connectivity to cloud services.

Amazon Route 53 (route53)

Amazon Route 53 provides managed Domain Name System (DNS) web service. Amazon Route 53 connects user requests to infrastructure running both inside and outside of AWS. Customers can use Amazon Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of their application and its endpoints.

Amazon SageMaker (sagemaker)

Amazon SageMaker is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes the barriers that typically "slow down" developers who want to use machine learning.

AWS Secrets Manager (secretsmanager)

AWS Secrets Manager helps customers protect secrets needed to access their applications, services, and IT resources. The service enables customers to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

AWS Security Hub (security)

AWS Security Hub gives customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. With Security Hub, customers can now have a single place that aggregates, organizes, and prioritizes their security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. Findings are visually summarized on integrated dashboards with actionable graphs and tables.

AWS Server Migration Service (SMS)-(sms)

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for customers to migrate thousands of on-premises workloads to AWS. AWS SMS allows customers to automate, schedule, and track incremental replications of live server volumes, making it easier for customers to coordinate large-scale server migrations.

AWS Serverless Application Repository (serverlessrepo)

The AWS Serverless Application Repository is a managed repository for serverless applications. It enables teams, organizations, and individual developers to store and share reusable applications, and easily assemble and deploy serverless architectures in powerful new ways.

AWS Service Catalog (servicecatalog)

AWS Service Catalog allows customers to create and manage catalogs of IT services that are approved for use on AWS. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, and helps customers achieve consistent governance and meet their compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

AWS Shield (shield, DDoSProtection)

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

Amazon Simple Email Service (ses)

Amazon Simple Email Service is an email service that allows customers to send transactional email, marketing messages, or any other type of content. The main Amazon SES sending components are the frontend request router, backend control planes for feature configuration and access management, and a sending Mail Transfer Agent (MTA). Customers can also use Amazon SES to receive messages. The main Amazon SES receiving components are the receiving MTA, backend control planes for feature configuration and access management, and a rule-based message processor.

Amazon Simple Notification Service (sns)

Amazon Simple Notification Service is a web service to set up, operate, and send notifications. It provides developers the capability to publish messages from an application and deliver them to subscribers or other applications. Amazon SNS follows the "publish-subscribe" (pub-sub) messaging paradigm, with notifications being delivered to clients using a "push" mechanism.

Amazon Simple Queue Service (sqs)

Amazon Simple Queue Service offers a distributed hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can move data between distributed components of their applications that perform different tasks, without losing messages or requiring each component to be always available. Amazon SQS allows customers to build an automated workflow, working in close conjunction with Amazon EC2 and the other AWS infrastructure web services.

Amazon Simple Storage Service (s3)

Amazon Simple Storage Service provides a web services interface that can be used to store and retrieve data from anywhere on the web. To provide customers with the flexibility to determine how, when, and to whom they wish to expose the information they store in AWS, Amazon S3 APIs provide both bucket and object-level access controls, with defaults that only permit authenticated access by the bucket and/or object creator.

Amazon Simple Workflow Service (swf)

Amazon Simple Workflow Service is an orchestration service for building scalable distributed applications. Amazon SWF enables developers to architect and implement these tasks, run them in the cloud or on-premise and coordinate their flow.

Amazon SimpleDB (sdb)

Amazon SimpleDB is a non-relational data store that allows customers to store and query data items via web services requests. Amazon SimpleDB then creates and manages multiple geographically distributed replicas of data automatically to enable high availability and data durability.

AWS Snowball (snowball)

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple and secure.

AWS Snowball Edge

AWS Snowball Edge is a 100TB data transfer device with on-board storage and compute capabilities. Customers can use Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local datasets, or to support local workloads in remote or offline locations. Snowball Edge connects to customers' existing applications and infrastructure using standard storage interfaces, streamlining the data transfer process and minimizing setup and integration.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. Customers can transfer their Exabyte data via a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration.

AWS Step Functions (states)

AWS Step Functions is a web service that enables customers to coordinate the components of distributed applications and microservices using visual workflows. Customers can build applications from individual components that each perform a discrete function, or task, allowing them to scale and change applications quickly.

AWS Storage Gateway (storagegateway)

The AWS Storage Gateway service connects customers' off-cloud software appliances with cloud-based storage. The service enables organizations to store data in AWS's highly durable cloud storage services: Amazon S3 and Amazon Glacier.

Amazon Systems Manager (ssm)

AWS Systems Manager formerly known as "Amazon EC2 Systems Manager" and "Amazon Simple Systems Manager", gives customers the visibility and control to their infrastructure on AWS. AWS Systems Manager provides customers a unified user interface so customers can view their operational data from multiple AWS services, and allows customers to automate operational tasks across the AWS resources.

AWS Transfer for SFTP (transfer)

AWS Transfer for SFTP is a fully managed service that enables the transfer of files directly into and out of Amazon S3 using the Secure File Transfer Protocol (SFTP)—also known as Secure Shell (SSH) File Transfer Protocol.

Amazon Translate (translate)

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Amazon Translate allows customers to localize content - such as websites and applications - for international users, and to easily translate large volumes of text efficiently.

Amazon Virtual Private Cloud (Amazon VPC) (ec2)

Amazon Virtual Private Cloud enables customers to provision a logically isolated section of the AWS cloud where AWS resources can be launched in a virtual network defined by the customer. The VPN service provides end-to-end network isolation by using an IP address range of a customer's choice, and routing all of their network traffic between their Amazon VPC and another network designated by the customer via an encrypted Internet Protocol security (IPsec) VPN.

AWS WAF (waf)

AWS Web Application Firewall is a web application firewall that helps protect customer web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Amazon WorkDocs (workdocs)

Amazon WorkDocs lets customers store all their files on one service. Users can share files, provide rich feedback, and access their files on WorkDocs from any device. WorkDocs encrypts data in transit and at rest, and offers powerful management controls, active directory integration, and near real-time visibility into file and user actions. The WorkDocs SDK allows users to use the same AWS tools they are already familiar with to integrate WorkDocs with AWS products and services, their existing solutions, third-party applications, or build their own.

Amazon WorkLink (worklink)

Amazon WorkLink is a fully managed service that lets the customers provide their employees with secure, easy access to their internal corporate websites and web apps using their mobile phones. With Amazon WorkLink, employees can access internal web content as easily as they access any public website, without the hassle of connecting to their corporate network.

Amazon WorkMail (workmail)

Amazon WorkMail is a managed business email and calendaring service with support for existing desktop and mobile email clients. It allows access to email, contacts, and calendars using Microsoft Outlook, a browser, or native iOS and Android email applications.

Amazon WorkSpaces (workspaces)

Amazon WorkSpaces is a managed desktop computing service in the cloud. Amazon WorkSpaces enables customers to deliver a high quality desktop experience to end-users as well as help meet compliance and security policy requirements.

AWS X-ray (xray)

AWS X-ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-ray, customers/developers can understand how their application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-ray provides an end-to-end view of requests as they travel through the customers' application and shows a map of the application's underlying components. Customers/developers can use X-ray to analyze both applications in development and in production.

Service Commitments

AWS communicates service commitments to user entities in the form of Service Level Agreements (SLAs), customer agreements (https://aws.amazon.com/agreement/), contracts or through the description of the service offerings provided online through the AWS website. More information regarding Service level agreements can be found at https://aws.amazon.com/legal/service-level-agreements/.

At the customer level, AWS has also implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified and to notify customers of potential operational issues that could impact the customer experience. A Service Health Dashboard is available and maintained by the customer support team to alert customers of issues that may be of broad impact. Current status information can be checked by the customer on this site, or by subscribing to an RSS feed to be notified of interruptions to each individual service. Details related to security and compliance with AWS can also be obtained on the AWS Security Center and AWS Compliance websites.

System Requirements

AWS communicates its system requirements to user entities and how to get started with using the AWS services in the form of user guides, developer guides, API references, service specific tutorials, or SDK toolkits. More information regarding the AWS Documentation can be found at https://docs.aws.amazon.com/. These resources help the customers with architecting the AWS services to satisfy their business purposes.

AWS has identified the following objectives to support the security, change, and operational processes underlying their service commitments and business requirements. The objectives ensure the system operates and mitigates the risks that threaten the achievement of the service commitments. The objectives below provide reasonable assurance that:

- Data integrity is maintained through all phases including transmission, storage and processing.
- Procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.

- Policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- System incidents are recorded, analyzed and resolved.
- Changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.
- Critical system components are replicated across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.
- Controls are implemented to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.

People

Amazon Web Services' organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing the Company's tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, security practices, policies and procedures. Employees are provided with the Company's Code of Business Conduct and Ethics and additionally complete annual Security & Awareness training to educate them as to their responsibilities concerning information security. Compliance audits are performed so that employees understand and follow established policies.

Data

AWS customers retain control and ownership of their own data. Customers are responsible for the development, operation, maintenance, and use of their content. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. All decommissioned hardware is sanitized and physically destroyed in accordance with industry-standard practices.

Availability

AWS is architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. These strategies include engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning.

Contingency plans and incident response playbooks are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business and the AWS Resiliency Program is annually reviewed and approved by senior leadership.

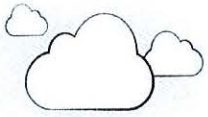
AWS has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple availability zones; authoritative backups are maintained and monitored to ensure successful replication.

Service usage is continuously monitored, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, AWS maintains a capacity planning model to assess infrastructure usage and demands.

Confidentiality

AWS is committed to protecting the security and confidentiality of its customers' content, defined as "Your Content" at https://aws.amazon.com/agreement/. AWS communicates its confidentiality commitment to customers in the AWS Customer Agreement. AWS' systems and services are designed to enable authenticated AWS customers to access and manage their content by design through tools that allow customers to determine where content is stored, secure content in transit or at rest, initiate actions to remove or delete content, and manage access to AWS services and resources. AWS has also implemented technical and physical controls designed to prevent unauthorized access to or disclosure of content.

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' content. AWS monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.



HOSTING, SECURITY, AND PRIVACY

HOSTING & SECURITY

The SchoolMessenger solution proposed for Suffolk County Community College is fully hosted Software-as-a-Service model and carefully engineered to ***meet or exceed industry best practices and collocated with a Tier III data center subject to annual ISO 27001 audits.*** In addition, at Intrado, our approach to information security, as well as our policies and procedures, are heavily governed by the information security framework outlined in ISO 27002. In short, our hosting facilities provide world-class enterprise hosting infrastructure with data protection, and security as a standard part of our service offering.

MULTIPLE DATACENTERS	All components of the application reside in multiple geo-dispersed datacenters (all SAS 70 Type II certified). Plus, it has redundant connections to the telephone grid. And, information is synchronized at every location. This means that even in the unprecedented case of a regional event affecting any part of the country, servers at the other locations continue processing notifications without interruption.
DUAL DELIVERY METHODS	We use multiple Tier 1 Voice Telecommunications Networks and delivers messages using best-of-breed VoIP, TDM, SMS, and email technologies. This is another way that we ensure the application has no single point of failure.
MULTIPLE, SECURE FACILITIES	For physical hosting we are proud to partner with multiple leading Internet co-location companies – the same outsourced IT partners employed by important content and enterprise customers. These facilities are protected by rigorous physical and biometric security systems. All sites are engineered to survive natural disasters. Plus, redundant network, power, HVAC, and fire detection/suppression systems ensure the highest levels of system availability.
INDEPENDENT SERVICE	The application and network were built from the ground up over several years and with sizable investment. We do not resell someone else's service. We own and operate the entire application. This means you never have to worry about the dependability of a third party.
HIGH CAPACITY	Our massive capacity allows users to send hundreds of thousands of calls in minutes. On average, we utilize less than 2% of our available capacity, and grow this capacity as needed based on usage. This helps ensure that during periods of peak activity (or even a regional emergency) the service can handle the needs of the College.

UNSURPASSED TRANSPORT ENCRYPTION	With SchoolMessenger solutions, all session information (including data exchanges between College systems and the service) is protected by 256-bit SSL encryption certified by Norton Secured, Powered by VeriSign, the trusted industry leader in secure certificate authentication services. They provide the highest level of encryption available to civilians in the US. This means that sensitive information like phone numbers and email addresses is fully protected.
PROTECTION FROM MULTIPLE REDUNDANT FIREWALLS:	The service uses redundant firewalls from two independent industry-leading manufacturers to provide double the protection and ensure high availability. A security flaw in one firewall layer doesn't compromise the system – or your data. The application uses firewalls with: - Integrated Deep Inspection for application-level attack protection for our Internet facing protocols, applied on a per-policy basis - Denial of service protection to protect against both internal and external attacks. - High-availability capabilities to minimize the potential for a single point of failure - Dynamic routing support to reduce reliance on manual intervention to establish a new route in the event of failure.
SECURE PASSWORDS	Passwords are stored securely and log in access is governed by industry standard encryption. Combined with the rules-based Web-browser access that limits each user based on data view restrictions, we provide a multi-point security schema that protects data from unauthorized use.
CONGESTION MANAGEMENT	The system consistently contacts large audiences very quickly; however, if the area receiving the calls can't handle all those calls, sending them at once will only overwhelm the phone network. That's why we utilize a unique Congestion Management Algorithm to maximize call delivery. Calls are delivered into any geographic area without overloading the local telecom infrastructure. This means your notification goes out efficiently and effectively.
BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN	SchoolMessenger has established a framework for both Business Continuity and Disaster Recovery Planning. Business Continuity addresses the sustainment of business operations in the context of a comprehensive approach to include migration strategies, capabilities, and processes. The Disaster Recovery Plan outlines the processes by which the business will resume after a disruptive event such as an earthquake, flood, or even a

	virus attack. These plans are communicated, exercised, maintained, and refreshed on a periodic basis.

PRIVACY

Student data is among an institution's most sensitive information. And it's imperative that this data be fully protected. We understand that. That's why we have taken all commercially available measures to protect your data.

Highlights Follow:

- **Privately Owned and Operated:** SchoolMessenger applications have been built from the ground up over several years and with sizable investment. As opposed to simply being a reseller of someone else's service, we own and operate our hosted notification service; other than intermediary phone companies and long-distance providers, there are no third parties involved in the transport of notifications.
- **Comprehensive Privacy Policy**: As per the SchoolMessenger privacy policy, ***no data is ever shared with any outside party for any reason***. Key provisions follow:
    - We do not sell, trade, loan or lease any information or data about our customers to any third party. Your contact information, the contact information of your constituents, your communications, data, documents, and information are completely private and fully protected against unauthorized access.
    - We are not a source of nor do we deliver unsolicited e-mail, unsolicited voice mail, or unsolicited faxes. We will not send any unwanted communication to you or your constituents.
    - We do not sell or otherwise provide information to direct marketers or any other third parties.
    - We do not disclose any non-public information about you, except as required or permitted by law. Under U.S. law, there is an affirmative duty of service providers to the public to report to the Federal Government's Cyber Tip Line knowledge of facts or circumstances of online child pornography. In the above events, Intrado, in its sole discretion, reserves rights of disclosure to others.
- **We maintain a comprehensive hiring, training, and retraining process which includes rigorous pre-employment screening.** Pre-employment screening can include but is not limited to:
    - Conducting credit referencing and criminal background checks
    - Verifying academic and professional qualifications

  - Undertaking detailed employment reference checking, including confirmation of employment dates, job titles, leaves (where relevant) and salaries

- Confirming current, past, and disqualified certifications and licenses, if any

- **Additionally, each employee, as part of the hiring process, signs agreements and statements** including but not limited to:
  - Non-disclosure agreement
  - Confidentiality agreement
  - Company policy acknowledgement and agreement
- **Student Privacy Pledge Signatory**: We are a signatory of the Student Privacy Pledge, which requires us to adhere to 12 stringent standards as a further assurance of our commitment to protecting your data. These include the following commitments:

STUDENT PRIVACY PLEDGE COMMITMENTS	
✗ Not collect, maintain, use, or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.	✓ Collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher, or the parent/student.
✗ Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.	✓ Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties.
✗ Not sell student personal information.	✓ Support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.
✗ Not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the	✓ Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

STUDENT PRIVACY PLEDGE COMMITMENTS

use of student personal information that are inconsistent with contractual requirements.	
✗ Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.	✓ Require that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information.
✗ Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student	✓ Allow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

SCHOOLMESSENGER AND FERPA COMPLIANCE

From Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)[1]: Education institutions may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, the institution must tell eligible students about directory information and allow eligible students a reasonable amount of time to request that the school/institution not disclose directory information about them. The institution must notify eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a bulletin, student handbook, or newspaper article) is left to the discretion of each institution.

INFORMATION SHARING EXCERPT FROM SCHOOLMESSENGER PRIVACY POLICY

The information we collect is not sold, traded, leased, or loaned to any third parties, ever. Only Intrado's SchoolMessenger employees who need access to the information in order to do their jobs have access to it.

- We do not sell, trade, lease, or loan any data about our members to any third party, ever. Your contact information, the contact information for all your constituents, your communications and your documents are completely private and fully protected against unauthorized access;
- We do not send any unsolicited e-mail, unsolicited voice mail or unsolicited faxes;
- We do not sell information to direct marketers or any other third parties. We do not distribute information to any third parties except as may be required to relay or deliver messages to your intended recipients; and,
- We do not disclose any non-public information about you, except as required or permitted by law.

Under U.S. law, there is an affirmative duty of service providers to the public to report to the Federal government's Cyber Tip Line knowledge of facts or circumstances of online child pornography. In the above events, Intrado, in its sole discretion, reserves rights of disclosure to others.

[1] http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

d) Anticipated Issues and Resolution

Anticipated Issues and Resolutions – Describe anticipated issues that your Company may encounter when performing the services required in this RFP and identify proposed solutions, including, but not limited to any significant deviation from previously agreed-upon work plans and reasons for the delay;

- ✓ Not applicable. Unlike other vendors who will be proposing an unknown product or service, ***we've served Suffolk County Community College with the exact notification services called for in this RFP since 2014.*** Upon award of the RFP, service will continue uninterrupted, but we'll evaluate your current use of the system to help make sure you're getting the most out of your investment. As this would be a simple renewal, this would not need a full implementation; this entire process would involve only a few hours of the College's time.

End of Text for Exhibit D

EXHIBIT E

Payment Terms and Conditions

1. General Payment Terms

a. Contractor shall prepare and present an invoice to the College for payment by the College. Invoices shall be documented by sufficient, competent and evidential matter. Payment by the College will be made within thirty (30) days after approval by the College.

b. Contractor agrees that it shall be entitled to no more than the fees set forth in this Exhibit E for the completion of all work, labor and services contemplated in this Agreement.

c. The charges payable to Contractor under this Agreement are exclusive of federal, state and local taxes, the College being exempt from payment of such taxes.

d. The acceptance by Contractor of full payment of all billings made on the final approved under this Agreement shall operate as and shall be a release to the College and/or County from all claims and liability to Contractor, its successors, legal representatives and assigns, for services rendered under this Agreement.

2. Agreement Subject to Appropriation of Funds

This Agreement is subject to the amount of funds appropriated and any subsequent modifications thereof and no liability shall be incurred by the College and/or the County under this Agreement beyond the amount of funds appropriated for the Services covered by this Agreement.

3. Limit of College's Obligations

The maximum amount to be paid by the College as set forth on the cover page of this Agreement shall constitute the full obligation of the College in connection with this Agreement and any matter arising therefrom.

4. Specific Payment Terms and Conditions

See, ATTACHMENT 1, Contractor's Cost Proposal, annexed hereto.

ATTACHMENT 1
Contractor's Cost Proposal

V. COST PROPOSAL

RFP No. R20-002

V. COST PROPOSAL

a. Proposers shall submit a cost proposal that includes all fees associated with the annual license, implementation, support, and training.

b. Proposer should provide all information it deems necessary to explain or clarify its Cost Proposal inclusive of any additional supplementary services, if available.

THANKS TO SUFFOLK COUNTY COMMUNITY COLLEGE'S CONTINUED TRUST IN OUR SCHOOLMESSENGER NOTIFICATION SERVICE, INTRADO HAS EXTENDED BEST-IN-NATION PRICING.

- ✓ Unlimited service included;
- ✓ Professional setup and data integration included;
- ✓ Technical Support included; and,
- ✓ Extensive training included.

SCHOOLMESSENGER PRICING BASED ON 20,000 STUDENTS	YEAR 1	YEAR 2 & BEYOND
SchoolMessenger – Fully Hosted Notification Services • ***$1.00/student/year***	$20,000	$20,000/year
Implementation and Project Management Services	$0	$0
Unlimited Online Training and 24/7/365 Customer Support • ***Unlimited online training for ALL your staff for the life of the contract*** • ***Unlimited 24/7/365 customer support for ALL your staff***	$0	$0
TOTAL	**$20,000**	**$20,000/year**

** No hidden charges or fees. No charge for version upgrades. No charge for staff.*

c. Description of payment schedule/structure/due dates for the duration of the Agreement.

- ✓ SchoolMessenger Communicate is licensed based on an annual per student fee. There are no additional costs for staff members.

  At the contract's anniversary, a yearly review is performed to ensure that the College is being charged for the actual number of accounts in use. This ensures that the College will not be trapped paying for unnecessary accounts no longer in use if enrollment decreases.

End of Text for Exhibit E

EXHIBIT F

College's Request for Proposals

The College's Request for Proposals (RFP) for Mobile Communications System Purchase, Implementation and Training services, issued October 24, 2019, together with any Addenda issued thereto, is incorporated herein by reference as Exhibit F.

End of Text for Exhibit F

EXHIBIT G

Contractor's Proposal

Contractor's Proposal, submitted December 11, 2019 in response to the College's RFP is incorporated herein by reference as Exhibit G.

End of Text for Exhibit G