

ALERT NOTIFICATION SYSTEMS “Build versus Buy”

OVERALL CONSIDERATIONS

The generally accepted criteria for a successful alert notification system (ANS) are that it must be available in times of crisis; support multi-modal notification; and do so quickly, accurately, and reliably. Universities and colleges debating whether to build or buy an alert notification system will benefit from the information that follows.

The components of an effective alert notification system are:

- A) Ability to send SMS text messages
- B) Ability to send e-mail messages
- C) Ability to originate voice notifications
- D) Ability to trigger downstream alerting systems via RSS or other triggers

The following must be taken into account:

- I. **Reliability and Redundancy.** Generally in-house solutions are located in an on-campus data center. Power loss and network connectivity problems render the alerting system useless without redundant, off-site facilities. If the institution does have an off-site backup, it must mirror the main site. In essence, institutions that build their own alert notification system must double the infrastructure investment. Additionally, a single hosting center relying on a single network or power provider is problematic. A Tier IV hosting center should be used, with redundant network, power, and cooling facilities.
- II. **Authentication.** In-house solutions often rely upon a centralized identity management and single sign-on solution. If that approach is taken, the identity management and SSO systems become a point of failure. They require the same redundancy and off-site mirroring as the alerting system. Otherwise, administrators will not be able to log and use it. For that reason, a stand-alone authentication solution is often desired, at least for administrators.
- III. **User and List Management.** The solution will need the capability to enroll users and provide ongoing management of their credentials. This goes beyond the

information often collected in a student information system, and will usually require support for multiple e-mail addresses, mobile numbers, and landline contacts per registrant. Furthermore, most solutions require the ability to notify subsets of the recipients (rather than sending all messages to “all”), so some form of group and list management will be required.

- IV. **Roles Based Access Control.** At a minimum, institutions will have 2 (two) categories of users – those who can send alerts and those who can’t. Often, more granular management of permissions is desired whereby allowing some administrators to send to just certain lists, or separating user-management privileges from alert sending privileges. In addition, two user-facing sites are required, one for end users (alert recipients) and one for administrators.
- V. **Reporting.** In an emergency, it’s important to confirm that the message is sent such that some ability to examine real-time reporting is required.
- VI. **Security.** The system must be impervious to hacking, a malicious party who is able to trigger a broadcast alert can send people into harm’s way intentionally. Therefore, third party security auditing is recommended. Personal information must be stored in accordance with FERPA requirements.
- VII. **Performance.** The system must be able to support rapid notification. Throughput measured in messages per minute is extremely important. Leading commercial systems are able to deliver at the rate of 25,000+ SMS messages per minute, by way of example. 2-way messaging support is desirable so recipients can respond with help requests or incident details (i.e. “flood waters are rising in the library, please cut the power!”) .
- VIII. **Monitoring & Alarming.** Emergency alerting systems are not used daily, therefore it’s easy for a failure to go unnoticed. For that reason, extensive and comprehensive system monitoring is required to ensure all equipment (firewalls, routers, servers, databases) are available and functioning as expected. When failures are detected, an alarming and response system and support procedure is required to ensure 5 9’s scale reliability.

DELIVERY CHANNEL CONSIDERATIONS

I. **SMS Delivery.** SMS can be sent 3 ways as follows:

- A. SMS via E-Mail (SMTP): SMS can be delivered by addressing messages as [phonenumber]@[carrierdomain.com]. This method requires accurate carrier information for all recipients in order to keep up with number ports. While this method is free, it is unreliable as the top 5 carriers accounting for 90%+ of mobile numbers actively SPAM block and throttle this communication method. For instance, if you exceed an unpublished threshold with Verizon Wireless for too many messages sent in too brief a period of time, your sending domain is locked out for 3 hours. At this point, if you blast again then you are locked out for another three hours. For this reason, SMTP-based solutions are not considered a viable emergency communication option for Tier 1 carriers.
- B. SMS Forwarding Service: Several SMS forwarding services exist that charge “per message” to deliver messages commercially using a shared “short code.” Unfortunately, these providers only support one-way communication which means that contacted parties cannot respond. In addition, their customer base tends to be dominated by marketing firms and “one-off” reminder traffic, so they generally do not have emergency-grade throughput. Messages will arrive, but it may take well over an hour to get all delivered.
- C. SMS Aggregator: SMS aggregators are the “industrial strength” providers that handle commercial SMS traffic and carrier-to-carrier message traffic. SMS aggregators will require the institution to lease their own commercial short code for sending SMS messages. These shortcodes are only available from one source. They cost \$6000 per year for a random number and \$12,000 per year for a “vanity” number that spells a word of your choice on a phone dial. In addition, the aggregators generally require a setup fee of approximately \$1,500 - \$5,000, and a monthly minimum traffic volume payment of \$1,500 - \$5,000. Once the short code is provisioned, it must be registered with each intended carrier and comply with CSC rules and regulations. Registered short codes are audited at least quarterly by the carriers, and perceived non-compliance would need to be researched and responded to. Aggregators offer different spans of carrier coverage (not all carriers are covered), and offer different throughput rates with the carriers. Available throughput range from 10 messages/second with a single connection, to 150 messages/second depending on the aggregator and the agreed upon monthly fee. Higher speed is more expensive. Interfacing with the aggregator is done via web services or SMPP transceivers.

Aggregators and SMS forwarding services in the United States cover different spans of carriers, but none cover Tier 3 carriers that include Helio, Cricket, Tracphone, Metro PCS, etc. For this reason, support for SMS via SMTP is required for all 3rd tier carriers, even if option (b) or (c) above is selected. It is worth noting that in the United States none of the SMS Aggregators have more than a single data center for bulk SMS traffic. They are all a single point of failure and experience outages. It's critical to contract with more than one delivery provider, and build in the ability to "fail over" from one to the other during a downstream outage.

- II. **E-Mail Delivery.** Many students opt not to use their school-supplied e-mail account as their primary. For that reason, most emergency solutions allow students to provide "preferred e-mail addresses" such as those from Hotmail or Gmail. In an emergency, Hotmail or Gmail may respond to the institution's e-mail blast as a SPAM attack and blacklist the institution as a sender (independent of a separate business relationship with these providers). The institution will need to be concerned with anti-spam countermeasures such as "tarpitting." Tarpitting grabs the SMTP sending threads and holds them for exponentially longer periods of time until a denial of service condition.
- III. **Voice Alerting.** Voice alerting is desired for members of the campus community who do not use text messaging, and for persons with disabilities unable to read text messages. In order to deliver voice calls quickly, a high level of available capacity is required. Until it's used, it unfortunately remains idle. Voice calling strategies must take into account that most of the institution's target community is served by local equipment. Given this, consideration must be given to not place too many calls too quickly whereby creating an "all circuits busy" condition.