Implementing a Crisis Communication and Personnel Accountability (PA) System

Best Practices and Lessons Learned

by Rear Admiral Bob Day, US Coast Guard (ret)

Former Coast Guard CIO and Cyber Commander

Principal, Bob Day & Associates LLC

In times of crisis, how do government agencies alert, advise, account for and determine status of their employees and rapidly relay this critical information to senior leadership?

Top of mind for many emergency management and HR federal agency executives: how to effectively initiate and manage communications during a crisis or contingency situation. Specifically, looking back at real-world examples such as the Navy Yard and LAX shootings, the ability to communicate with and account for all staff employees and contractors remains a challenge that many executives are striving to solve – particularly given the increasing potential for events of this nature and other phenomena (weather, earthquake, fire) to occur.

As threats against the US and its government increase, we must enable solutions that can immediately reach and account for all staff and empower agency leadership to respond and report status of their personnel as required by federal mandate.

Today, many federal agencies have developed or acquired PA capabilities to meet the requirements of Federal Continuity Directive 1 and the continuity planning mandates specified in NSPD-51/HSPD-20. The directive specifically requires that all departments and agencies must have "a capability to account for all personnel" and "the means and processes in place for employees to contact their organization in a timely manner."

Many organizations developing their overall continuity and resilience plans quickly realized that a PA capability is a critical element because, in most cases, personnel are truly the mission-essential capability that contributes to agencies' National Essential Functions (NEFs).

Many organizations have implemented some form of crisis communications system that usually includes alerting – and some may have included accountability functions, too. The reality: both are needed and, to be highly effective, they need to be tightly integrated and feature alerting to reach people via multiple communication modes within minutes and real-time capture, to enable accountability data and robust and granular reports.

Gone are the days of call trees and manual accounting for staff; to keep pace with the information demands during crisis/response situations, organizations must leverage the extensive technology available today to effectively alert and account for workforce. Organizations that have conducted in-depth crisis communications planning and implemented modern integrated alerting and accountability systems have demonstrated significantly improved performance when challenged with crisis.

A 2014 NeNez survey of 201 enterprises ranging in size from 250 to 5000 employees found that organizations that develop and frequently exercise their crisis communication plans and capabilities are:

- Able to notify personnel twice as fast
- 55% more likely to resolve emergencies within one hour
- Less likely (13% less) to suffer monetary losses than organizations that did not develop detailed crisis communication plans

This paper presents best practices/lessons learned for planning and implementing a crisis communication and accountability system, examined through the lens of the U.S. Coast Guard's experience.

The genesis of our journey for accountability began with emerging requirements for accountability of the CG workforce staff during hurricane season and other crisis situations. Lessons learned from events such as the Hurricane Katrina, the Deep Water Horizon Oil Spill and California wildfires drove our commitment to augment our already robust alerting system with accountability features. We wanted to avoid any development, customization or integration beyond what is considered COTS/GOTS, given the frequency of events.

Further, time was of the essence since the next hurricane season or crisis would be rapidly upon us. After extensive analysis, we discovered the tools and system needed were readily available to address this vital need.

Based on my personal experience as CIO during planning and implementation of a successful Coast Guard PA capability, I learned some valuable lessons that can assist organizations to truly maximize the overall effectiveness of a crisis communication and PA system. Our experience also shows that an effective implementation enables further expansion of scope to cover core capability used for everyday command and control, yielding even a greater return on investment.

Lesson 1: Requirements Definition

It all starts with the initial planning for a crisis communications system that can readily support the PA application. Make no mistake; you must have the ability to alert all employees within minutes to enable any effective accountability functions. Specifically, an effective PA system must:

- Reach all constituents of an organization
- Enable accountability functions, including status of an individual and an assessment ability that automates the tracking of each accountability case from start to finish
- Efficiently work across a broad range of communication mediums
- Enable the accountability data to be displayed in varying formats desired by the broad range of potential users (think Geographic Information System [GIS] and reporting dashboards)

But if you dig further into the requirements for your PA system, you'll find numerous other capabilities that are absolutely essential as your system matures and its use throughout the organization becomes ingrained into daily practices. You have to really think through all of these things, because many of these capabilities are extremely hard to quickly "bolt on" to a basic system after you have already rolled it out into the organization.

These capabilities include:

- An up-to-date, complete and accurate user repository with all possible user contact details
- The ability to initiate and manage communication processes at multiple organization levels, as applicable to the situation – from campus-wide to nationwide
- The capability to leverage multiple communication modalities to not only alert personnel but also collect their response and status
- Real-time aggregation of the responses collected from all mediums and present unified information to the decision makers at all levels of the organization
- The ability to develop and store predefined alerting/communication templates to enable quick alerting/communication initiation when a crisis happens
- The flexibility to update and customize the communication messages, methods and processes if needed
- The ability to provide a robust, secure, and accountable process for not only soliciting inputs from personnel, but allowing them to report their status in an unsolicited manner – including allowing personnel to report status for others who may not have access to a communication capability
- Collecting a broad range of data such as needs assessment, availability to support, location and intentions

The definition of "requirements" really comes down to storyboarding the entire accountability cycle that your organization is trying to establish; the who, what, why and how for all of the various crisis and contingency scenarios that you believe your organization must be prepared to respond to.

I would also suggest that organizations think beyond just crisis/contingency communications and evaluate how the system can be used to enhance day-to-day command and control; I explain this in more detail at the end of the paper.

It is also critical to assess the communications capabilities and preferences of your workforce, since these vary greatly by demographics and are constantly shifting. A 2013 Center for Disease Control survey showed that two out of every five Americans have discontinued their landline and rely solely on a wireless phone. Additionally, younger workers tend to do much of their communication by text and social media versus voice phone calls. A successful implementation absolutely requires detailed understanding of your workforce's communication preferences.

The storyboarding and discovery discussed above will require engagement and input from a broad group of stakeholders, which leads me to Lesson Number 2.

Lesson 2: System Owner

In most organizations, I have seen the sponsorship for PA assigned to the Chief Human Capital Officer (CHCO) which, at first glance, seems logical. Although the CHCO is the perfect champion for the effort, a matrix team comprised of representatives from all organizational elements (especially CIO, Emergency Management Teams and leads from core operating business lines) is absolutely necessary for the success of the initiative.

At USCG, the Executive Oversight Committee (EOC), comprised of the leadership from all business lines, provided this matrix input to the CHCO lead for the project. This type of engagement allowed all organizational entities to have a full discussion and understanding of the complexity of crisis communications and the overall organizational contingency plan which PA would support.

Representation from field organizations, especially operating units who will likely be the predominant users of the system, proved absolutely critical to the overall success of the effort; engagement of this personnel sparked the initial thoughts about how the system could also be used to support local and regional command and control needs.

Planning for a PA capability will very rapidly start focusing on identifying the organizations authoritative source for the personnel data needed by any PA system. Most organizations have numerous potential sources for personnel data – e.g., pay systems and active directory – but settling on the "authoritative" source having the most relevant and up-to-date information communication channels (work and home email, home and work phone, mobile phone) is key.

The USCG PeopleSoft Human Resources system called Direct Access proved to be the system of choice. Furthermore, during planning it was recognized that having employees update their contact information in Direct Access at least annually would be a critical success factor. Strategies were developed to "force" an annual update of employee information and to monitor such updates per unit.

Lesson 3: Protect Agency PII Data

Given the sensitivity of the Personally Identifiable Information (PII) needed by most crisis communication systems to conduct alerting and record assessment, the implementation team had to make some challenging decisions on how the system would access and use this data. Ultimately, the USCG decided to retain this data behind USCG firewalls which – given the recent concerns with cyber security – has proven to be a smart choice.

In short, the USCG could not allow storage of any USCG PII data at any location external to the USCG firewall. Recent breaches and hacking attempts/successes across the federal and private sectors solidified our decision to protect our PII and ultimately our employees' privacy. As organizations develop their systems, their cross-functional team should discuss security concerns with the Chief Information Security Officer to determine the appropriate safeguards as well as where PII should be stored. Organizations considering cloud solutions for crisis communications really have to do some deep assessments with respect to the security provisions of the provider and the physical location of the hosting service.

Lesson 4: Deploy a System That Meets an Organization's Needs

With an enterprise strategy and requirements agreed upon by all stakeholders and a viable authoritative data source, the implementation team quickly sought a technical solution that met core requirements. Since 2009, the USCG Data Center in Martinsburg, WV (called Operations Systems Center [OSC] Martinsburg) had been successfully using AtHoc, Inc.'s Interactive Warning System (IWS) for a broad range of alerting needs like Emergency Response Group (ERG) notifications and operational alerting to both USCG and maritime sector personnel.

The demonstrated ability of the AtHoc IWS to provide all of the requirements that I listed in Lesson 1 clearly aligned with a majority of the needs identified by all stakeholders. Specifically, the capability to allow multiple levels of the organization (from HQ to regional commands) to not only initiate alerts and communications but also customize them to the region's specific needs and leverage multiple communication modes (phone, email, text, fax, and smartphone application) for not only alerting but for receiving responses.

The USCG and AtHoc then identified the Navy's SPAWAR Personnel Accountability and Assessment Solution (PAAS) as a proven GOTS capability to address the accountability, assessment, inclusion of employee dependents and case management functions and information display requirements. The combination of AtHoc IWS and PAAS allowed the USCG to leverage existing capabilities at OSC Martinsburg – keeping the PII behind our firewalls and monitored by USCG Cyber Command – and rapidly deploy a solution that was already proven by many of our DOD partners.

This also negated any development or integration, as the two systems had already achieved integration and leveraged the best-of-breed COTS and GOTS solutions available today. The combined solution is also deployed at the Dept. of Veterans Affairs, where it supports 500,000 employees. This solution was adopted and deployed by the USCG, culminating in the highly successful USCG PA Solution known as CG PAS.

Lesson 5: Use the Right Personnel and Set Them Up for Success

The USCG implementation project team designated contacts in each of its districts (operational commands within specific regions) and established "champions" to support CG PAS deployment. These champions helped the project build the various alert groups that the operational commander believed were necessary for their area of operations; the groups ranged from all personnel within the entire district to subsets, either tied to a mission function or smaller geographic region. Having the flexibility to tailor the solution to the desires of the operational commander was key to rapid acceptance and use, and having a local "champion" to assist the project team to understand and build these requirements proved to be essential.

The USCG also found that having on-site training and assistance to tailor the build and ensure that personnel were comfortable with the system streamlined the time needed to roll out the full capability. A district-by-district roll-out strategy also proved to be a smart move, and allowed the implementation team to focus and ensure success for each district.

Maintaining frequent contact with the local "champions" and training their replacements has proven to be absolutely essential to ensure that the system data stays relevant and operational commanders fully understand how to leverage the system locally.

Lesson 6: Get the Most from the System

When a crisis communication and accountability system is leveraged properly, it has a positive impact across the organization, provides leadership immediate visibility and greatly assists command and control because response personnel have timely information on the status of the workforce. With a little creativity and some additional capability, the USCG PAS system and especially AtHoc IWS provided us much more than just crisis communications and PA. As we leveraged it, we realized how effectively it can directly contribute to command and control of daily operations.

USCG missions require a highly mobile workforce: marine inspectors travel daily throughout the ports in their area and even internationally, maritime safety and security teams are frequently deployed in broad range of geographic regions, aircraft crews deploy throughout their area of responsibility, and support professionals are constantly in the field providing maintenance services. These mobile workers require the PAS system to be capable of alerting simultaneously to multiple communication channels since it is difficult to know which channel will be available to them at any given time.

Operational and support commanders, especially in crisis situations or an operational response, constantly want to know "where my troops are and what their readiness status is." A capable PAS can provide the operational commander with the ability to quickly query subsets of personnel for status or, better yet, have the mobile worker equipped with a smartphone enabled with PAS compatible applications that leverage the real-time location service on the phone.

PAS capabilities also form a useful predefined dispatching mechanism. In this scenario, predefined personnel are identified as being part of a standard response plan to a situation. This list is then preprogrammed in the PAS and alerts are sent out via multiple communication channels upon activation by the command center. Gone are the days of the paper recall list and the phone calls with no response.

The possible uses are endless; it just requires that operational commanders and/or management understand the PAS system and link the capabilities to their operational plans and then frequently exercise them.

Lesson 7: Engage with the Community

The alert and warning capabilities of a solid PAS system can enhance communications with your partners, stakeholders and affiliates in the public and private sector. With a multi-modal communication capability, organizations can engage a broad range of organizations and personnel; especially the public, when you leverage social media forums.

For example, Coast Guard Captains of the Port (COTPs) in almost all CG regions have leveraged AtHoc IWS as a primary means for alerting both public and private stakeholders in each major US port on changes to Maritime Security Conditions (MARSEC) based on threat information being received from national sources. But use of the system has expanded to communicating a broad range of maritime alerts and non-emergency information (e.g., waterway closure).

Leveraging these capabilities to expand the reach and overall capability of your system to enhance command and control will require some advanced thought with respect to what those situations would be, who to contact and what means should be leveraged to send out alerts and receive responses. Organizations should consider predefined recipients and communications templates that can be rapidly tailored for a specific situation, to save time in the heat of the moment if a crisis does occur.

AtHoc is also rolling out a new capability called Connect that will provide even greater capability and flexibility for alerting and two-way communication between parties in a community of interest like a major port, and even those in the supply chain for their partners. I will develop a future best practices paper on how I believe this capability can significantly enhance interoperability between partners and other organizations.

Summary

The primary goal of this paper has been to provide the reader with the insight and lessons learned from my experience with the Coast Guard team that implemented what has become the CG enterprise system leveraged by all levels of the organization to not only provide a highly effective PA capability, but also enhance internal and external communications for both crisis and routine command and control, and provide an interoperability channel to our many stakeholders. Organizations of all sizes should consider the best practices outlined here in developing a crisis response plan, developing an alerting and PA system that can keep personnel safe in the event of a disaster and enhancing command and control for day-to-day operations.

About the Author

Rear Admiral Robert E. Day Jr., US Coast Guard (retired) was the Assistant Commandant for Command, Control, Communications, Computers and Information Technology, Chief Information Officer and Commander of Coast Guard Cyber Command from July 2009 until July 2014.

During his 34-year career, he held a broad range of communications and information technology leadership positions responsible for acquiring, operating and maintaining the myriad of advanced capabilities used by the Coast Guard to execute their extensive missions.

Rear Admiral Day holds a BS in Electrical Engineering from the US Coast Guard Academy and a MS in Telecommunications Systems Management from the Naval Postgraduate School in Monterey, California. Currently, he's the Prinicipal at Bob Day and Associates LLC.