**Add to report**

**Community Feedback**

In order to understand to understand the organizational needs, specific pain points, and overall challenges in emergency responder community, we conducted a series of expert interviews with first responders. We asked the following questions:

1. How are different organizations are approaching?”
2. What kinds of digital and in person credenitals FR's are using?
3. What kinds of websites and mobile applications FR's are using for work?
4. How much friction exists accessing digital resources?

We gained access to contacts through a senior project team member with contacts in the community.

Between May and July 2017, we conducted interviews with the following:

* Eric Epley, Strac: <http://www.strac.org/>
* Dave Smith: Director of EMS for San Marcos, Texas
* Kharley Bagley Smith, Emergency Services Director, Hays County, Texas
* Ken Bell, Governor’s First Responder Advisory Committee, Rowlett Fire Marshal’s Office as a Deputy Fire Marshal

Emerging key themes as follows:

1. SMART cards are not being used! Chips are on the cards, yet not being scanned because no device is readily available. Points to the viability of a mobile device – even if not all responders carry them, key people at check-in do have.
2. Security is an ongoing issue.

With the chaos, threat, and uncertainty that accompany such disasters, allowing unauthorized people to access an emergency site not only puts them in danger, but may endanger fellow emergency responders. Conversely, turning away qualified people is also a problem.

As David Smith explained:  **“I’m always worried. It’s a best effort on our end. What we use it’s a private AT&T cloud. Everything is routed back into my CISCO system.”**

1. Validation of credentials is important issue for safety.

Kharley’s story about first responders during flood in 2015 not having proper training: “People were seriously injured. They would not have been assigned that task if we knew,”

1. Current practice is inefficient

In a crisis situation accompanied by chaos and threat, these manual system of t-cards, passport systems, sign in rosters, and smart cards are wholly inadequate for confirming the essential details about an emergency responder, namely their skills, credentials, and authorizations.

As David Smith explained

* Issuing of badges: **“Problem with badge is the physical aspects. Your badge is everything — physical identity is tied to that….how does it expire. Once you lose it, you have to order. what happened to the others?”**
* Updating **– “There’s a big hole. There’s [no other option] out there — credential reset take a long time. Can’t lose it. What makes it real? No one is storing those credentials in a centralized place. If they lost it - revoke it, reissue it, doesn’t exist.**

1. Lack of standards

* Lack of standards-- As David Smith explained: **“If there is no push to adopt the standard, it won’t happen…it has to be put out at a federal level. Right now there’s no common standard for third parties to write to that standard.”**
* Decentralization -  **“Applications are out there, they are just not tied together. At some point there has to be some agreement, this is what they have to meet. I don’t see another solution. There needs to be a standard — a federal standard.**

The consequences of a fragmented and outdated system are highly problematic for the first responder themselves as well for the entire emergency community. There are, as one first responder said, “No other options out there.” The lack of a solution puts at risk the safety, security, and accessibility to first responders who are qualified.

1. Mobile Device
2. Adoption Barriers
   1. Culture
   2. Source of directive

We are in the process of contacting the following:

1. Mobile PD: <http://gomobilepd.com/>
   1. Writes a mobile app for 100 police departments, including Austin.
   2. Initial feedback is that identity infrastructure at PD's is messy.
2. Mark43: <http://www.mark43.com>
3. Peter Alcock [peter.alcock@mark43.com](mailto:peter.alcock@mark43.com)
4. Evidence.Com
5. John Wandelt, Nief: <https://nief.org>
6. .Anthony Buck, State Emergency Responder
7. Joseph Leonard, Coast Guard Emergency Responder
8. Christopher M. Piehota Ph.D.

Interview Protocol

I. QUESTIONS ABOUT END USER

1. Person / Organization Tell us about the purpose of your organization? What is your role? What is the size and structure of your organization?

2. IT staff: Is there a dedicated IT staff? Is there IT staff dedicated to user and access management? ----

II. IT STAFF PERSON WHO IS RESPONSIBLE FOR USER MGT

Tell us about identity practices?

a. In rough terms, how many usernames and passwords (or other types of authentication) do you have? What are some of the systems people need to access? Does your organization have a single sign-on system that provides access to multiple websites?

b. (IT Question) Do you know where the organization stores usernames and passwords?

1. Microsoft Active Directory

2. SaaS Identity Provider (Okta, OneLogin, Microsoft Azure, Google, Salesforce, other SaaS)

3. Other LDAP (Sun, Oracle, IBM, CA, OpenLDAP)

4. Relational database (MySQL, Postgress, Oracle, MS SQL)

5. Other: please explain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Does the first responder have a smart card that complies with federal standards? Can you share your thoughts on these credentials? Do you think usage should be extended to more people? What are some of the challenges for issuing more smart cards (or using them)?

5. What would you think about a mobile identity card for first responders?

6. Do you think people in your organization would object to using to using their person smart phone to apply for a first responder mobile identity card?

7. When responding to a large, multi-jurisdictional disaster, can you share your thoughts or concerns about the process for identifying people either in person, or when they use certain digital tools (mobile applications, websites)? 8. Are there standard certifications that you think would be important to convey via the mobile identity card. Is interoperability an issue? 9. Can you share your thoughts about using credentials other then passwords (or smartcards) to access websites or mobile applications? 10. What are the most important organizational applications that your organization sees the need to upgrade within the next five years?