SOCIAL NETWORKING FOR THE POLICE ENTERPRISE
An In-Depth Look at the Benefits, Requirements, and Challenges of Establishing a Social Networking Platform for Law Enforcement

Major Cities Chiefs Association
Developed in support of the Criminal Intelligence Enterprise (CIE) initiative, and in partnership with the Major County Sheriffs Association, the MCSA Intelligence Commanders Group, and multiple Federal partner agencies.

By: Dori Koren
D9007K@lvmpd.com
LETTER FROM THE CHAIR

LAS VEGAS METROPOLITAN POLICE DEPARTMENT
OFFICE OF THE SHERIFF

October 14, 2013

On behalf of the Major Cities Chiefs Intel Commanders, I want to take this opportunity to introduce the attached overview of Enterprise Social Networking and its impact on intelligence sharing. Many of you know, over the past few years, the Major Cities Chiefs Intel Commanders Group have been working very hard on creating sound policies, procedures and practices in order for all of us to better share this critical information. In the development of this document, they themselves spent time evaluating the impact of the social networking platforms, and how they can be utilized to entice members within our profession to become even more active in the sharing process of day to day criminal activity, day to day data as well as intelligence.

Attached, you will find an overview of what the Intel Commanders Group feel is important for us, within our profession, to evaluate prior to embarking on an Enterprise Social Networking platform. There have been a number of drafts circulated throughout the Intel Commanders Group at Major Cities Chiefs as well as at Major County Sheriffs.

This product before you today is the final version. Many edits have been made, modifications to include critiques and criticism from many of the Intel Commanders. I for one, as the Chair of the Major Cities Chiefs Homeland Security Committee, welcome any and all feedback of any reviewers of this particular document that you may have. I want to personally thank the Major Cities Chiefs Intel Commanders Group for making this publication a reality.

Douglas C. Gillespie, Sheriff
EXECUTIVE SUMMARY

Scope: The emergence of social networking technologies has transformed the way people interact, develop social ties, exchange information, and organize their personal and professional lives. As a result, Enterprise Social Networking (ESN) platforms—which offer organizations a closed Facebook-like program to increase connectivity, reduce costs, and enhance productivity—are on the rise in both business and government. This report explores the benefits, requirements, and key challenges for implementing such a platform for the law enforcement and homeland security community. The judgments and findings are based on existing literature, extensive research, the evaluation of numerous software systems, and the consolidated perspective of 77 law enforcement leaders from 45 major agencies.

Background: In June 2011, the Major Cities Chiefs Intelligence Commanders Group (MCCICG) began working on developing a proactive approach for enhancing the effectiveness, efficiency, and appropriateness of locally-led intelligence operations. This national effort, identified as the Criminal Intelligence Enterprise (CIE) initiative, was unanimously approved by the Major Cities Chiefs Association (MCCA) in October 2011, and later adopted by the Major County Sheriffs Association (MCSA) in January 2013. One of the key objectives of the CIE initiative is to enhance law enforcement connectivity by establishing a secure social networking environment that emulates the proven and well-recognized Facebook program. This vision is what sparked and fueled this effort and ultimately the research that is presented in this report.

Key Findings

Establishing a secure social networking platform for law enforcement is not only innovative and attractive but it also advances crime-fighting, enhances information sharing, and improves succession planning.

- Its use would help combat the complex problems of crime and terrorism, which has become increasingly dependent on interconnecting the law enforcement community. Violent gang members, pimps, prostitutes, robbery crews, drug distributors, and other criminal syndicates frequently transcend state and national borders. To effectively counter this issue, law enforcement must stay ahead and leverage social networking technology to enhance police connectivity and collaboration.

- It would enhance information sharing by fostering professional relationships. People are more likely to share information with those that they can relate to and as such, enabling your personnel to foster more social ties with their colleagues from within their home agency, as well as from other agencies, will result in more cooperation.

- It would improve succession and knowledge-sharing by establishing a community memory that can then be tapped into by others as agencies mature and evolve. In particular, the loss of expertise that accompanies the increasing rate of turnover would be offset by providing employees with a means for capturing the knowledge that is commonly “in their head”, and sharing it with the rest of the organization.

A Facebook-like social networking platform for law enforcement would provide tremendous value and cost savings.

- It would increase the efficiency of police operations by reducing email communication, de-conflicting duplicative efforts, and increasing productivity.

- It would enable personnel to develop and maintain their professional relationships as they progress through their careers, encounter new contacts, and even retire from their organization.
- It would help in detecting crime trends and potential organizational problems by providing our personnel with the ability to scan live streams of information, news feeds, and the activities of their colleagues, from any location, at any time.

- It would provide another means for developing leadership through Social Network Analysis, which can help identify who carries influence, facilitates teamwork, and advances or prevents progress within an organization.

The MCCA “Social Networking Needs” survey, which included 77 law enforcement and homeland security leaders from 45 major agencies, revealed that:

- 69% believe a secure social networking platform for law enforcement would enhance information sharing.

- 78% believe that the development of a secure social networking platform for law enforcement is important.

The Copbook pilot proved successful in evaluating the potential for establishing a social networking platform for law enforcement, and identifying the specific needs for implementing such a platform nationally.

- Beyond the traditional social networking tools, the Copbook platform proved to have some valuable features. The platform has a pre-established strategic partnership with the National Law Enforcement Telecommunications System (Nlets), it offers an attractive brand name, is fully customizable, and is based on simplicity.

- An evaluation of the first 30 days of the Copbook pilot showed a consistent increase in both user adoption and content development. The most valuable information exchanged included comments regarding current events such as the Boston terrorist attack; status updates, which included what users were doing during a given period of time; and requests for information on agency procedures and tactics.

<table>
<thead>
<tr>
<th>Productivity</th>
<th>Efficiency</th>
<th>Morale</th>
</tr>
</thead>
<tbody>
<tr>
<td>79%</td>
<td>94%</td>
<td>77%</td>
</tr>
<tr>
<td>Of 77 L.E. leaders already use Facebook for personal and/or professional purposes.</td>
<td>Of 800 L.E. agencies surveyed by the IACP report using public social media in some way.</td>
<td>Of business and IT leaders say their companies are using social collaboration.</td>
</tr>
<tr>
<td>87%</td>
<td>87%</td>
<td>87%</td>
</tr>
<tr>
<td>Of companies worldwide already have a presence on Facebook and Twitter.</td>
<td>Of IT leaders report using Enterprise Social Networking (ESN) successfully.</td>
<td>Of business end-users were more productive with enterprise social networking tools.</td>
</tr>
<tr>
<td>72%</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>Of all online adults use at least one social network.</td>
<td>Of business end-users said ESN increased their productivity, speed, and happiness.</td>
<td></td>
</tr>
</tbody>
</table>
While promising, the pilot version of the Copbook platform also had multiple deficiencies. The platform did not increase the amount of relationships users had prior to the pilot, nor did it show any significant increase in the frequency of information being shared. This was due to three correctable issues: the size of the pilot group was too small to spark the addictive connectivity that usually accompanies social networking; the user profile component lacked the ability to post information directly to the user; and limited mobile access prevented consistent use of the platform.

The far majority (73%) of pilot participants stated a post-pilot version of Copbook that was expanded to the larger law enforcement community would be useful. Additionally, the number of participants that described their access to information from other major law enforcement agencies as “easy”, increased by 10% after the pilot.

Although the pilot version of Copbook proved to be inadequate as a permanent solution, the trial allowed us to identify the specific needs and modifications that would enable success. Based on this evidence and with the proper modifications, the Copbook platform could prove to be an effective solution for establishing a secure social networking platform for law enforcement.

In addition to piloting Copbook, several other information sharing platforms and social networking solutions were reviewed or considered. Although user-access was limited in some cases, a variety of sources were used to help identify proven practices and potential challenges. Based on this initial research and the opinions that were expressed by some of the members of the MCCICG, it appears that most pre-existing and emerging platforms, to include Copbook, have yet to adopt many of the necessary principals that enable social networking to flourish. This should not come as a surprise considering that only 20% of ESN platforms actually succeed in the workplace. To help guide the development of current platforms and future efforts, the following considerations should be taken into account:

- The platforms that attempt to provide too many features tend to lack in simplicity. Ensuring simplicity does not only involve providing the user with an easy-to-navigate platform but it also means fulfilling specific needs, while not cluttering the platform with so many “bells and whistles”.

- Enterprise Social Networking efforts for law enforcement should emulate Facebook more than any other social networking site. This is not only important because Facebook is the most prominent in establishing connectivity but also because it’s familiar design will nearly eliminate the need for training new users.

- While some information sharing platforms also offer social collaboration tools, their potential for social networking is usually restricted by the need for security. Some of these platforms also struggle in adopting users and as such, would not serve as an effective means to launch new social networking tools.

- Since the far majority of law enforcement professionals spend their time in an unclassified environment, and since social networking is dependent on continuous access; a classified social network would likely be ineffective.

- If a platform’s expected revenue is dependent on advertising or product sales, then it is possible that the contents of the platform could be influenced by advertisers, and that user information could be used for commercial purposes.

- Merging pre-existing platforms should be considered as a future possibility. The current budget climate makes it difficult to justify separate but similar efforts and more importantly, most of the user-base that would be expected to partake in any of these platforms would derive from the same over-arching community.
Based on the findings of this report, establishing a national and secure social networking platform for law enforcement would prove very useful and likely transformational. The following are three options that should be considered by the MCCA and MCSA:

- **Option 1 – Adopt a Modified Version of Copbook:** If modified as proposed and with built-in flexibility, a post-pilot version of the Copbook software could prove to be an effective solution. In this option, each agency would agree to purchase membership to the platform separately. Access to the program would cost a large-sized agency approximately $24,000 annually which would include use for every employee of that agency. The annual membership model would allow agencies to adopt the software on a tentative basis so that they could further evaluate its usefulness before permanently committing. If most agencies cannot afford to purchase the platform at this time, the MCCA and MCSA should consider working with Federal partners to help fund or subsidize such an effort.

- **Option 2 – Pilot Additional Platforms:** Another option would involve conducting additional pilot programs to determine whether other platforms possess the potential for establishing a social networking platform for law enforcement. While an out-of-the-box version of any of the pre-existing platforms would likely not work, customizing one of these solutions after a successful pilot could offer some potential.

- **Option 3 – Formalize and Acquire Support:** The third option is to propose an MCCA and MCSA resolution that supports establishing a social networking platform for law enforcement. The resolution would help formalize the need and solidify the requirements that are outlined in this report. In turn, this would help attract support from partner agencies and it’ll motivate vendors to modify their platforms to fit our specific needs. The formation of an executive task team to lead this effort would be just as important. Such a team would help acquire the needed funds through grants or other means; make a final determination on the best platform and vendor; and facilitate adoption across all MCCA and MCSA agencies.

Regardless of the option selected, the research and recommendations in this report should serve as a guide for moving forward. We have a limited number of opportunities to capture the commitment of our end-users before they begin to disengage and classify every new effort as someone’s “pet project”. Therefore, it is critical that we spend the time and resources to evaluate the right approach early on. The enabling and inhibiting attributes that are outlined on pages 22-25 will serve as a framework for doing this.

**Socially Driven Connectivity**

One of the most vital elements to social networking is the ability to look into the lives of our friends, maintain this view, and compare ourselves to their progress. As social beings, we’re naturally curious about how and what other people are doing, and in particular our friends and co-workers. Most of us also tend to measure our growth by comparing ourselves to others. This is why Facebook users often find themselves clicking and navigating through profile after profile, exploring the lives of those that interest them. This blend of curiosity and competitiveness is what fuels the addictive nature and success of social networking. By incorporating this concept in a social networking platform for law enforcement, we too, form a healthy addiction to connectivity.
INTRODUCTION

Social networking technologies continue to indiscriminately take root and even the critics who once viewed social networking as a trend for the younger generation, have now come full circle. According to the Pew Research Center, 72% of all American adults that use the internet use at least one social network, and over half of all of these users are now over the age of 35. Most people now spend more time on Facebook than any other website; and YouTube, Twitter, LinkedIn, and so many other social networking sites continue to take center stage. Whether it be identifying a common interest, establishing a new friend, or receiving breaking news; people now rely on their social network to process the world they live in.

Beyond individual use, most organizations from across different industries are also looking to harness the power of social networking for the work place. Almost all Fortune 500 companies, to include IBM, Sears, GE, and Toyota; now have a presence on Second Life and other social networking sites\(^3\), and numerous government agencies continue to explore the potential of social media for their missions. Social media’s proven ability to spark revolutions, influence elections, drive business, and interconnect over a billion people from across the globe, has attracted the attention of nearly every industry.

The law enforcement community is no exception. Most agencies have already adopted social networking for community outreach and many have recently begun exploring the use of social networking for undercover operations and investigations. Social media strategies and policies are also on the rise. In 2009, the International Association of Chiefs of Police (IACP) launched the “Center for Social Media”, and later released guidance regarding law enforcement’s use of public social networking sites. The Criminal Intelligence Coordinating Council (CICC) also released guidance on developing social media policy in February 2013, and then reinforced it in the 2013 National Criminal Intelligence Sharing Plan (NCISP). Most recently, the Police Executive Research Forum (PERF) published a forward-leaning report on law enforcement’s use of public social media sites for investigations and the gathering of information.

While progress has certainly been made, law enforcement’s use of social networking for **internal purposes** and **organizational development** remains unchartered territory. Determining whether a secure social networking platform for the law enforcement enterprise would enhance police operations, increase morale, and reduce inefficiencies is emerging as the latest hot topic. Many law enforcement executives are now inquiring about this potential and more and more vendors that offer social networking solutions are quickly surfacing to try and fill this need.

In an effort to explore this potential and establish a framework for success, this report presents the key challenges, benefits and requirements of implementing a successful social networking platform for the law enforcement and homeland security enterprise. The judgments and findings presented are drawn from existing literature, extensive research and the consolidated perspective of personnel from many of the member agencies of the Major Cities Chiefs and Major County Sheriffs associations.
The core properties of a social networking platform are: Profiles, Friends, and Comment Structures. The profile is where a person presents his or her identity, the friends are the person’s self-defined social network, and the comment structures serve as a means for communicating, collaborating, adding content, and receiving information.

There are two general types of social networking platforms: Public social networking, which is the use of publicly available sites such as Facebook and Twitter; and Enterprise Social Networking, which is the use of private social networking sites for the workplace.

**Public Social Networking**

Public social networking platforms possess a dynamic ability to connect people, content, and processes through a single system. The most notable are Facebook, Twitter, MySpace, and LinkedIn. The value of public social networking is no longer up for debate. In the business world it has become standard practice. In fact, 87% of companies worldwide have a presence on Facebook and Twitter; and 80% of small-to-medium businesses plan to increase their use of social media this year.27

The use of public social networking sites has also become widespread within the law enforcement community. In a 2012 study conducted by the International Association of Chiefs of Police, 94% of the 800 law enforcement agencies that were surveyed said they use public social networking in some way, and 56% of those that are not using it are considering its adoption in the near future.17 Most recently, the Police Executive Research Forum (PERF) released a report entitled “Social Media and Tactical Considerations for Law Enforcement”.28 Offering valuable guidance on law enforcement’s use of social media for public outreach, managing major events, obtaining intelligence, and conducting investigations; the report highlights how prevalent this topic has become for the law enforcement community. It also shows how the public has begun to “expect” law enforcement agencies to have an online presence on social networking sites.

<table>
<thead>
<tr>
<th>Law Enforcement Leaders Using Public Social Networking Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facebook</strong></td>
</tr>
<tr>
<td><strong>MySpace</strong></td>
</tr>
<tr>
<td><strong>Twitter</strong></td>
</tr>
<tr>
<td><strong>LinkedIn</strong></td>
</tr>
<tr>
<td><strong>Google Plus</strong></td>
</tr>
</tbody>
</table>
Enterprise Social Networking (ESN)

The success of public social networking sites has sparked the development and rapid growth of Enterprise Social Networking (ESN) for the workplace. ESN refers to social networking sites that are designed for the enterprise or a closed community, which emulate much of the functionality of public social networking sites (i.e. “a Facebook for Cops”). Estimated to be a $6.4 billion industry by 2016, ESN platforms are on the rise as many companies, organizations, and communities look to capitalize on the value of social networking in the workplace. Ranging from NASA, the Intelligence Community, and the Department of Homeland Security, to health care providers, the business sector, and educators; many have already implemented or piloted ESN platforms for their organization. In fact, the technology research company Gartner predicts that by 2016, “50 percent of large organizations will have internal Facebook-like social networks, and that 30 percent of these will be considered as essential as email and telephones are today.”

In a study conducted by Forrester, the majority of IT-Decision-Makers (87%), business leaders (68%), and end users (68%), from 500 organizations, said they use ESN platforms. Of those end users, 55% said that their use of an ESN platform increased their speed, productivity, and happiness at work. Specifically, and of interest to law enforcement, ESN platforms have proven to save organizations money by reducing email communications, preventing duplication, increasing morale, and enhancing productivity.

ESN Success Stories

- **Toronto Police Services:** In July 2011, the Toronto Police Service (TPS) officially launched its social media program which not only included a strategy for public outreach and investigations, but also for improving internal communications. Having already been regarded as “one of the most forward-thinking law enforcement users of interactive digital tools in the world”, the TPS has truly pioneered the use of social networking, particularly for outreach, prevention, and investigation. Although their use is more centered on public social networking sites such as Facebook and Twitter, their efforts have certainly demonstrated the potential of social networking in the workplace. Their results have included “more productive and meaningful interactions with communities and individuals” and increased efficiency.

- **Wells Fargo:** After seeing encouraging results in a pilot project focused on using social collaboration to boost sales, Wells Fargo is now moving ahead with plans to implement an enterprise social network for their organization. Having already tested Salesforce Chatter, Yammer, NewsGator and Socialcast; Wells Fargo is now piloting a custom ESN platform that’s based on Jive technology. The success of this new pilot is still to be determined but their early efforts have certainly proven that they are on the right track.

- **Hewitt Associates**, a human resources outsourcing and consulting firm, uses Facebook-style social networking to stay in touch not only with employees, but with former employees. Within the first four months of launching their platform, they had more than 2,600 alumni and retirees register for the site, which was double from what they expected. This connectivity has increased their potential in recruitment and relationship building.

- **Davies Public Affairs:** In an effort to address employee disaffection, the firm launched an enterprise social networking platform. Within weeks, employees were calling the platform the “single most useful tool within the organization, using it as their first stop in the morning to check the company’s activities”. The firm was able to facilitate more information sharing; connect employees to subject-matter experts to increase project efficiency, reduce paperwork, streamline operations, and increase areas of known specialization by about 300 percent.
The benefits of establishing an enterprise social networking platform for law enforcement are tremendous, but many agencies are unclear on the best path to take. Like many new technologies, social networking entered the government landscape at the grassroots level and is growing rapidly. As a result, executive-level awareness is limited and early efforts to implement social networking tools within law enforcement have been ad hoc and ineffective. To address this issue and evaluate the true potential for law enforcement; the demand, need, and value of establishing a social networking platform have to be identified, and the concerns must be evaluated.

The Demand

The following are the results from a survey of 77 law enforcement professionals, to include police chiefs, sheriffs, officers, and analysts, that represent 45 major law enforcement agencies:

- **70%** Believe having a secure social network for law enforcement would ENHANCE information sharing.
- **78%** Believe developing a secure social network for law enforcement to be IMPORTANT.
- **73%** Believe a secure social network would be USEFUL.

The Need

**Affect Crime and Terrorism**

The rapidly increasing complexity of crime and terrorism has redefined how law enforcement and homeland security agencies must collaborate. Violent gang members, pimps, prostitutes, robbery crews, drug distributors, and other criminal syndicates frequently transcend state and national borders. Identifying their presence is no longer as simple as looking for a particular indicator or group name. They co-mingle, change form, and operate across jurisdictions. They’re also quick to leverage new technologies and in particular social networking.

To effectively combat these issues, law enforcement must stay ahead and continuously develop new strategies and tools that enhance police connectivity, information sharing, and collaboration. Social networking platforms offer a dynamic ability to connect people and facilitate information sharing. Just as criminals and terrorists leverage this technology, so should law enforcement and homeland security practitioners.

This becomes especially important considering that law enforcement operates in a decentralized manner. Police personnel work different shifts and assignments from different offices and area commands, yet they must rely on each other to continuously share information, de-conflict operations, and coordinate their efforts.
Improve Succession and Knowledge-Sharing

Like many organizations, law enforcement agencies thrive on communication and knowledge-sharing. No individual person knows it all and to be effective, police personnel have to collaborate and leverage each other’s abilities. However, communication and collaboration among employees is rarely structured and almost never documented. Social networking helps offset this issue by establishing a community memory where ideas and knowledge can be maintained and leveraged indefinitely.

This becomes especially valuable when considering the inclining rate of retirements that many law enforcement agencies are now experiencing. Even with succession planning, many agencies suffer greatly when their most experienced and sometimes most knowledgeable make their departure. Much of the knowledge and expertise that took decades to develop is contained in the retiree’s head and it’s rarely transferred to others in the organization. An effective social networking platform serves as a mechanism that naturally captures knowledge from the experienced and transfers it into a community memory that can then be tapped into by others, as agencies mature and evolve.

Enhance information sharing

The downside of most current information sharing platforms is that they revolve around storing and transferring data rather than fostering connectivity. No matter how advanced a system may be, the user who is expected to input and share data is still more likely to do so if he or she knows who they’re connecting with. Social networking, which enables people to develop and manage their relationships, creates this needed connectivity which in turn fuels information sharing.

The Value

Increase Efficiency and Save Money

There is some persuasive research about the efficiency gains that accompany the use of social networking in the workplace. Some experts have even went as far as predicting that social networking will someday replace email as an enterprise solution for facilitating collaboration, teamwork, and knowledge sharing\textsuperscript{11, 23}.

Regardless of whether this proves true, early studies of social networking in the workplace certainly present some serious potential. A report by McKinsey Global Institute claims that business employees spend 28% of their workday answering, writing or responding to email.\textsuperscript{7} They also spend another 19% of the time trying to track down information and 14% collaborating with co-workers.\textsuperscript{7} Social networking has also begun to replace Google as the preferred method of search, and several innovative corporations have already begun adopting this technology as their primary method for disseminating internal information quickly and effectively.\textsuperscript{35}

With shrinking budgets and limited resources this potential has only become that much more relevant for law enforcement and homeland security agencies. Like many in the private sector, police personnel often fall victim to excessive emails, duplicating efforts, and spending too much time searching for information. Considering the gains seen in other industries, a social networking platform for law enforcement would prove quite useful in saving agencies time and resources.
Establish and Strengthen Relationships

Social networking stimulates professional exchanges and collaboration by allowing people to reveal personal information about themselves. As seen in any context, people like people like themselves, and when provided with a mechanism to foster ties based on shared interests, skills, or background; they can become more productive.

From a law enforcement perspective, a social networking platform would enable personnel to develop and maintain relationships as they progress through their careers. As an officer or analyst transfers assignments or promotes, they would be able to stay connected to their peers with limited effort. They would also be able to identify those that share common interests or who are working on similar efforts.

From a national perspective, the same personnel would be able to network and stay connected with their colleagues from other agencies. This connectivity would serve as a form of “social glue” that increases the quality of information that is shared both within an agency and between other agencies.

Identify Crime Trends

With social networking, people can actively scan their information streams for new trends and crime problems. For example, when officers across jurisdictions share that they are all investigating a series of copper thefts, the potential for a trend is revealed and those that share the same interest are now able to collaborate, exchange best practices, and coordinate solutions.

Develop Our People

Establishing a social networking platform would also enable organizations to better evaluate and develop their personnel. Leveraging Social Network Analysis, organizations can learn a lot about their employees to include identifying who carries influence, facilitates teamwork, advances the mission, or prevents progress.

Overcoming Concerns

Personal Use

Some police chiefs and sheriffs have expressed a concern regarding employees using a law enforcement-only social networking platform for non-work related discussions. For example, a user making a sports-related comment or discussing their vacation plans with their colleagues. The truth is social networking is intended to be social, and restricting it to only work-related content would contradict its purpose and prove detrimental to its success. Just as our employees socialize in person and through current technologies such as department phones, emails and texts; we should not expect them to operate differently in a social networking environment.

If anything, law enforcement agencies should encourage their personnel to get to know one another. When we personalize a relationship with a colleague, that association makes it infinitely easier to collaborate and work together to accomplish a mission. A law enforcement-only Facebook-like platform would facilitate this relationship building and enhance teamwork.
Over-Sharing

Social networking is based on openness and transparency. User profiles reveal personal information, interests and associations; and the connectivity that’s created by social networking usually results in more overall communication. While useful, the sensitivity that revolves around law enforcement operations can naturally present some hesitation to these results.

This same concern was shared by many Fortune 500 companies, the health care industry, and many others. Worried about employees inadvertently exposing proprietary information on a new technology could cost a company millions. Likewise, a health care provider that releases protected patient information could violate federal laws and face damaging lawsuits.

However, this concern, which is driven more by uncertainty than logic, has been proven to be invalid. The reality is that there are many safety measures that can be taken to minimize the inadvertent release of sensitive information, just as agencies do with current communication technologies. Also, while the risk of over-sharing can never be fully removed, the benefits of utilizing social networking in the workplace have proven to significantly outweigh the risks.

Inappropriate Use

Another similar concern revolves around employees posting inappropriate messages. While the potential exists, it has proven to be much less of an issue when compared to current outlets such as phones, emails, text messages, administrative messages, and radio communications. Social networking allows for distributed moderation, also known as "self-policing". Comments on a social networking platform are attributed to an author, so if something is inappropriate, the other users can quickly flag it as a problem. Ultimately, this transparency stands in stark contrast to other communication tools, where inappropriate content can sit for years.

Technology Overkill

Law enforcement leaders should be cautious about asking their personnel to try new systems too often. If we keep asking our employees to try a new technology platform that ends up failing, we begin to lose their trust and we shrink their appetite for trying new solutions. The truth is we have a limited number of opportunities to capture the commitment of our end users before they begin to disengage and classify every new effort as someone’s “pet project” or “thesis”. This is why it’s so important to spend the time and resources to evaluate the right approach early on. With the right planning, the right execution, and some selectivity, we’ll be more likely to succeed.
COPBOOK PILOT

Copbook is an Enterprise Social Networking (ESN) platform that is marketed specifically to law enforcement. As suggested by its name, Copbook is intended to emulate the proven and well-recognized Facebook program, exclusively for the law enforcement community. Like many ESN platforms, it is based on Jive technology, currently utilized by many agencies in the Intelligence Community. It offers users the ability to build a personal profile, connect with their colleagues, and communicate with their network.

In March 2013, the Major Cities Chiefs Association partnered with Copbook to pilot a prototype version of this software. As part of the Criminal Intelligence Enterprise (CIE) initiative, the primary purpose of this pilot was to evaluate the potential of a social networking environment for law enforcement and to identify the specific needs for developing a more permanent platform.

The pilot spanned 90 days and the test group was comprised of 163 users from the Major City Chiefs Association, Major Counties Sheriffs Association, National Fusion Center Association, and federal partners. The type of user ranged from police chiefs and sheriffs to officers and analysts from 54 major agencies from across the Nation and Canada.

To help test the effectiveness of the pilot and to identify what would need to be modified or included in a more permanent version, two forms of measurement were used. The first included an evaluation of the software and the usage during the pilot. The second involved surveying the participants both before and after the pilot.

Copbook Evaluation

In evaluating the software, we identified several features that proved useful and promising, as well as some deficiencies that would need to be addressed if Copbook was to be used beyond a pilot environment.

Promising Features

In addition to many of the traditional social networking features, the following are a list of the features that proved to be the most promising:

- **News Feed:** Like many social networking platforms, the Copbook experience revolves around the user’s news feed, which is a running log that displays the activity (posts, comments, and connections) that is related to the user’s network of friends. Although there were a few minor issues with the layout, the overall news feed feature proved to be quite useful.

- **Customizable:** One of the best aspects of Copbook is that it is not being proposed as an off-the-shelf solution. Instead, it is fully customizable, and the vendor appears to be flexible and interested in transforming Copbook to fit the specific needs of law enforcement.

FACTS

<table>
<thead>
<tr>
<th>163</th>
<th>18</th>
<th>42%</th>
<th>36%</th>
<th>54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of users that participated in the CIE Copbook Pilot</td>
<td>Average number of connections or “friends” each user developed.</td>
<td>Of users leveraged Copbook to identify an expertise that could be utilized by fellow users.</td>
<td>Of users uploaded a photo to their profile page.</td>
<td>Number of agencies that were represented in the Pilot.</td>
</tr>
</tbody>
</table>
**Nlets Partnership:** The Copbook platform has a pre-established strategic relationship with the National Law Enforcement Telecommunications System (Nlets). This provides the potential for hosting CJIS information without compromising easy access and functionality.

**Brand Name:** Copbook has an appealing, recognizable, and catchy brand name that clearly implies it is intended to be a “Facebook for cops”.

**Simplicity:** The Copbook platform does not attempt to burden the user with too many features. Instead, it presents itself exclusively as a social networking tool that can even be further simplified.

**Notable Deficiencies**

- **Profile:** The layout and functionality of the profile aspect of the Copbook platform was insufficient. The profile is divided into tabs rather than being a single page which makes it harder to navigate. More importantly, the profile lacks a "wall" feature, which would enable users to post information on each other’s profiles.

- **Mobile:** During the pilot, Copbook had released a mobile application for IPhone users but this was too far into the pilot to be fully evaluated. This also excluded Android and Blackberry users which made up most of the pilot user-group. The lack of mobile access likely served as one of the greatest hindrances to the pilot. Since users were unable to stay continuously connected, their contributions were limited.

- **Network Building:** The Copbook pilot lacked an effective mechanism to recommend relationships for new users. Although, the embedded feature entitled "Copbook Genius" was intended to automatically identify connections, its effectiveness is dependent on the size of the overall community. With a limited pilot group, this tool proved ineffective and as such, it was difficult for users to find other users that they wanted to connect with.

- **Too Small of a Pilot:** The user group proved to be too small to effectively trigger the flow of information that is commonly seen in a successful social networking platform. With only a 167 users, the pool in which users could identify new "friends" was very limited. Future pilot programs should seriously consider expanding to at least include all of the personnel of 2-3 agencies, in addition to a nationally representative body of several hundred other users.
Usage Evaluation

An evaluation of the first 30 days showed a consistent increase in both user adoption and content development. New users from the pilot group were joining each day and new content was being added on an increasing basis.

The average number of connections or "friends" each user developed within three months was 18. While seemingly mediocre, the pool in which users could identify new relationships was limited to only 167. In a post-pilot version, where the platform would be open to the entire law enforcement community, the number of connections or social reach would be expected to exceed 150.

42% of users leveraged Copbook to identify an expertise that could be utilized by fellow users, and 36% of users uploaded a photo to their profile page.

The frequency of comments was low, which was likely due to limited mobile access and the inability to post information on individual user profiles.

First 30 Days of the Copbook Pilot

Content Growth

2.6 Posts Daily

Content creation grew steadily during the first month.

Rate of Adoption

2.0 Users Daily

29 new users registered in the first day, with a total of 60 registering in the first month.
The content that was most useful included comments regarding current events such as the Boston terrorist attack; status updates which included what users were doing during a given period of time; and requests for information on agency policies and procedures.

**Example Posts**

**Jason Leavitt**
While stationed here in DC working at DHS, I’m glad to see the sovereign citizen movement is still a focus back home in Vegas. Al Salinas is right up front, and putting it out there for the media! [http://www.fox5vegas.com/story/22112068](http://www.fox5vegas.com/story/22112068)

**Share - Comment - Like (1) - Repost**

**David Azuelo**
We too have a very active Sovereign movement in southern Arizona, to include some very aggressive anti-law-enforcement tactics that they are employing along the US Mexico border. These groups...

**Like (1)**

**Dennis Richards**
Has anyone encountered organized mischief to their city’s camera initiatives? Nothing to date in Buffalo, NY...There are a number of websites promoting this “cause” including [http://earthfirstnews.wordpress.com/2013/02/26/contest-because-security-cameras-wont-destroy-themselves/](http://earthfirstnews.wordpress.com/2013/02/26/contest-because-security-cameras-wont-destroy-themselves/)

**Share - Comment - Like (1) - Repost**

**Jeffrey Rogers**
We looked into this and have found no known cases in the US. Seems to be overseas at this point, but we notified our investigation units in case they start seeing reports related to criminal mischief of cameras.

**Like (0)**

**David Azuelo**
Mass causality bombing at Boston Marathon. Secondary devices found according to the Department of Homeland Security. Check any sporting events in your local areas.

**Share - Comment - Like (1) - Repost**
Survey Results

In addition to evaluating the software and the usage, a participant survey was administered before and after the pilot. The survey was comprised of a series of questions which were intended to measure the connectivity, access, and functionality from the user perspective.

When asked how many established relationships with other major law enforcement agencies prior to the pilot: 45% said between 1-10, 30% said 11-20, 10% said 21-40, and 15% said 41 or more.

When asked how many professional contacts with other major law enforcement agencies prior to the pilot: 5% said between 1-10, 35% said 11-25, 35% said 26-50, and 15% said 51 or more.

While it’s unlikely that participants lost relationships as a result of the pilot, both of these areas were perceived to stay the same or decline by most pilot participants.

Prior to the pilot, 75% described their current accessibility to points of contacts and information from other major law enforcement agencies as EASY and 25% described it as DIFFICULT. After the pilot, the participants that described their accessibility as EASY increased to 85%.
Users also had the opportunity to provide written feedback regarding the pilot. This included both positive and negative remarks. The following graphic presents most of this feedback:

### ADDITIONAL FEEDBACK

1. **“I feel a service of this type has value and can be beneficial to our mission nationwide”** - Lieutenant
2. **“Great platform for socializing with LEO’s, sharing information, and making requests or asking general questions. Very intuitive”** - Commander
3. **“Too many systems being utilized by our center”** - Director
4. **“Copbook has great future potential as a tool for somewhat secure communication”** - Chief of Detectives
5. **“Fields and functionality were very limited. It has potential. I understand it was intended to be like Facebook in some regards but I think the pilot did not expand enough. By limiting it to nominated or verified law enforcement personnel only you might attract officers that might not be willing to use social media”** - Lieutenant
6. **“I like the Copbook forum. Not sure if it’s better than a direct email or phone call in certain situations. I do like it as a general information sharing type tool”** - Lieutenant
7. **“I like the concept, but other than adding and being added by others during the pilot there was not much else done with it. I sent one message to someone and they never responded via copbook”** - Sergeant

---

**Why Don’t We Just Use Facebook?**

The solution for most industries is to simply adopt the publicly available Facebook site for both internal and external use. However, the law enforcement community is a bit unique. While many law enforcement personnel utilize Facebook in their private lives, they tend to separate it from their work life. The primary reason is their need for some level of privacy. Associating themselves to law enforcement on a public social networking site may result in unexpected consequences. This is why a social networking site that emulates the proven Facebook technology but allows users to safely communicate regarding work-related and non-work related topics is desired by so many in law enforcement.
Enterprise Social Networking

The term Enterprise Social Networking (ESN) refers to software solutions that are presented specifically for the purpose of social networking in the workplace. In law enforcement, some of the early ESN efforts have been promoted as Facebook-like platforms for cops. However, based on our initial review, most of these pre-existing and emerging platforms, to include Copbook, may still fall a bit short from achieving such a reality. This should not come as a surprise considering that only 20% of ESN platforms actually succeed. To help guide the development of these platforms, the following are some approaches that have been identified as problematic:

- **Police Resource Websites with Embedded Collaboration Tools**: There are already several websites that strive to be a one-stop-shop for police connectivity and information exchange. Many of the original ones have adapted to the social networking craze and now offer some social collaboration tools as part of their construct. Most of the up-and-coming ones have evolved into what some would consider a “mash-up” of several of the more prominent social networking sites. In some cases, this could be a Facebook-like network that includes a Twitter-like communication tool and a YouTube-like video library. However, when platforms attempt to provide too many features, they tend to lack in simplicity. Ensuring simplicity does not only involve providing the user with an easy-to-navigate platform but it also means fulfilling specific needs, while not cluttering the platform with so many “bells and whistles”. Many of the ESN platforms that have failed in the private sector lacked in purpose. Rather than offering users a tool to fill a specific void, many companies attempted to offer their users an entire tool shed. This of course caused confusion and ultimately led to failure. The lesson to be learned is that a platform that is promoted as an end-all-be-all for networking, training, collaboration, shopping, and so on; may be less effective than one that serves a very specific purpose. It’s not that a company should never consider incorporating additional capabilities into their platform; it’s just that they should do so selectively and not until after they reach a critical mass of users.

- **Platforms that Deviate too much from the Facebook Design**: To be as attractive and as easy to use as the proven and well-recognized Facebook, companies should emulate Facebook. If social networking is truly the goal, then Facebook—which has proven to be the most attractive and most used—should serve as the primary example. There is difference in building a "LinkedIn for cops" verse a "Facebook for cops". While both may be useful, the latter is where the most potential lies. A LinkedIn-like platform would serve as a "virtual rolodex" for cops to find each other, whereas a Facebook-like platform would serve as a social utility for cops to manage their professional relationships and produce a dynamic-web of connectivity. Some may suggest that simply combining the two approaches would get you the best of both worlds but this too is unlikely.

- **Information Sharing Platforms with Embedded Collaboration Tools**: Sensitive But Unclassified (SBU) platforms are designed to facilitate information exchange within the law enforcement and homeland security community. While some of these platforms offer social collaboration tools as a secondary purpose, their potential for social networking is usually restricted. The security that is usually required for such platforms limits their flow of information and user access. For example, many of these platforms require compartmentalizing users into different communities, or only allowing users to log into the platform from a desktop computer. Unfortunately, these security needs hinder social networking.
Platforms that are Limited to a Classified Setting: Platforms that are on a classified network can be effective for users that spend most of their time in a classified setting. However, for most of the law enforcement community, this is not a likely scenario. The far majority of law enforcement professionals spend their time in an unclassified environment and usually in the field. This, in combination with the fact that social networking is dependent on continuous access, makes a classified social network an ineffective option for law enforcement.

Platforms that are Offered at No Cost to Law Enforcement: This approach, while unique and initially appealing, may present some new challenges. If a platform’s expected revenue is dependent on advertising or product sales, then it is possible that the contents of the platform could be influenced by advertisers, and that user information could be used for commercial purposes. This in turn may create some hesitation in the users that are uncomfortable in joining a platform that is not owned and operated by a government entity. However, if companies are able to overcome this concern and gain trust, this could prove to be an effective approach for achieving success during the current budget challenges.

Platforms that Focus Too Much on Organizing Users into Groups: For social networking to flourish and to grow organically, it must first reach a critical mass of users. To do so, users must have the ability to quickly find and connect with people they know and/or people they wish to collaborate with. As discussed later in this report, the groups feature—which many companies are quick to promote—can cripple this growth. While such a feature can prove to be useful down the road, encouraging users to compartmentalize themselves by agency or interest early on, can lead to silos of information. The better approach is to allow users to develop a personal network that is based on their sphere of influence rather than the groups they join or don’t join.

Platforms that Lack in Reputation: Some pre-existing platforms are plagued due to a long history of criticism. Despite revisions, many of these platforms continue to struggle with attracting and maintaining users. This lack of buy-in makes it very difficult to utilize such platforms to launch new social networking efforts.

While some of these practices are dependent on the manner in which they are applied and the environment in which they are executed in; most are likely to prove as lessons learned. At a minimum, further evaluating the good and the bad of these approaches will only help guide the development of a law enforcement social network. Merging pre-existing platforms should also be considered as a future possibility. The current budget climate makes it difficult to justify separate but similar efforts and more importantly, most of the user-base that would be expected to partake in any of these platforms would derive from the same over-arching community.

Software Race

Like most new efforts, there are many vendors that quickly emerge offering the “best solution”. Establishing a social networking platform for law enforcement is certainly no exception. In fact, the race has already begun and the competition is only expected to intensify in the coming months. As this occurs, it’s important that law enforcement leaders stay focused on the vision through the eyes of the end-user. Just as with any business, the users, or lack thereof, will make or break any endeavor. We could adopt the most sophisticated, innovative, and cost-effective software solution but if it fails to attract and retain enough users, it quickly becomes irrelevant. The right solution is out there but finding it without wasting resources will take some significant filtering and focus.
According to Gartner, a world-leading technology research company, 80% of Enterprise Social Networking platforms will not succeed. Most organizations apply the “provide and pray” approach which involves “providing access to a social collaboration technology and then simply praying that something good will come of it”. This of course proves ineffective and it illustrates the importance of adopting proven practices and avoiding the mistakes that many others have already made. As such, the following enabling and inhibiting attributes are provided as a framework for establishing a successful enterprise social networking platform for law enforcement.

Enabling Attributes

Emulate Facebook

The platform should closely resemble and function much like the proven and well recognized Facebook platform. There is a reason why internet users spend more time on Facebook than any other web site. It is simply the most appealing and effective design. Facebook dominates the social networking space with 98% of social networking users on Facebook; 29% on MySpace, 18% on LinkedIn and 13% on Twitter. Facebook also has the lead on daily use, with 52% of Facebook members using the platform daily whereas only 33% use twitter, 18% use MySpace, and 7% use LinkedIn on a daily basis. Above most all other enabling attributes, emulating Facebook is critical. It will ensure adoption, retention, and decrease the need to train users on how to use the platform.

| Top 8 U.S. Web Brands by Total Minutes, in Billions (Neilsen March 2013) |
|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| FACEBOOK                    | GOOGLE                     | YAHOO                       | YOUTUBE                     | AOL                         | MSN/BING                    | MICROSOFT                   | AMAZON                      |
| 58.4                        | 21.4                       | 20.7                        | 14.6                        | 10.9                        | 9.3                         | 4.1                         | 3.2                         |

Secure Yet Easily Accessible

The platform would have to be secure yet not to the point where it becomes difficult to access or utilize. Social networking is fueled by openness and the ability to connect with others. Restricting either results in a lack of adoption and/or a handicap to the flow of information. Platforms that compartmentalize users into groups, social circles, communities of interest, or special interests groups, tend to be less effective than the platforms that allow users to create self-defined, interconnected, and free-flowing networks.

Secure Hosting

Despite the need for openness, a reasonable level of security would still be required. A level or protection that is at least comparable to what is used to secure department email communications would normally suffice. However, since this effort expands nationally, the safest solution is to house the platform on a secure, reliable, and pre-existing national network.
Dependent on a Critical Mass

The success of a law enforcement social networking platform is dependent on obtaining a particular amount of core users that could serve as the "nucleus" for influencing growth. The exact threshold is unclear, but similar to any startup, a tipping point that attracts adoption is needed. Once that point is reached, the user-base would naturally and rapidly increase as individuals gravitate towards inclusion. In other words, the appeal for networking is weak when there are only 100 people in the network versus 100,000 people.

Mobile Access

The platform must include mobile access. Without an effective mobile application for Android, IPhone, and Blackberry operating systems, the addictive nature that accompanies social networking cannot be achieved. This is especially important considering that many expect mobile internet usage will surpass internet access from desktop computers by 2014\textsuperscript{19}.

<table>
<thead>
<tr>
<th>What Device?</th>
<th>I-Phone</th>
<th>Blackberry</th>
<th>Android</th>
<th>Tablet</th>
</tr>
</thead>
<tbody>
<tr>
<td>A survey of 77 law enforcement professionals from 45 of the largest law enforcement agencies revealed that I-Phone and Blackberry devices would be most commonly used to access a social network. Specifically, 36% said I-Phone, 27% said Blackberry, 20% said Android, and 17% said Tablet.</td>
<td>36%</td>
<td>27%</td>
<td>20%</td>
<td>17%</td>
</tr>
</tbody>
</table>

Individualized Privacy

Similar to Facebook, each user should retain control of who within the network can view or access each aspect of the information they post. This not only provides the user with the comfort of controlling their information but it also limits the risk of exposure should there be a breach by an unauthorized user. For example, if a user’s profile was breached, they should only have access to that specific user’s network of friends, rather than the entire user-base.

Publish and Subscribe Model

One of the greatest challenges of any information sharing or social networking platform is filtering out the white-noise. This is why simply on-boarding an entire community onto a platform proves ineffective and unappealing. Users want to select what they are informed about, who they connect with, and how they receive information. The most effective and proven strategy is the "Publish and Subscribe" model which allows users to manually build their network, publish information, and subscribe to their interests by "liking" or "following" specific posts.

Recommend Friends Feature

In addition to reaching a critical mass, the platform must also drive the rapid growth of each user's individual network. To do so, one of the most important enablers is having a feature that automatically identifies and suggests people on the network that a user may know. Another aspect of this feature would involve allowing users to invite friends to the network via email and other means.
Distributed Moderation or "Self-Policing"

Similar to many software systems within the private sector, the platform should leverage its user-base to identify inappropriate activity. A feature that allows users to “flag” or report content that they view as inappropriate, serves as an effective means for maintaining appropriateness and identifying violators.

Email Notifications

The platform should link each user’s account to an email address. This allows the user to receive email notifications when he or she receives a message or a request to be added as a friend. However, it’s equally important to ensure that notifications are limited and that the user doesn’t have the ability to respond to a message through their email. Too many email notifications will be viewed as spam and then ignored. And while having the ability to respond to a message from an email notification may seem like a good idea, the process tends to detract users from logging on to the platform. The solution is to have an effective mobile application that provides the user with notifications, as well as the ability to respond directly from within the platform.

Search for Common Interests

The platform should include a search tool that allows users to easily and quickly find other users who have common interests, as well as to search for other users by name, affiliations, and contact information.

Inhibiting Attributes

Poor Showing Initially

A poor showing or launch of any new technology before it can take root can be detrimental to its success. This is especially true for social networking platforms which are highly dependent on reaching a critical mass quickly. The platform must prove to be effective, valuable, user-friendly, easy to access, and appealing prior to any large-scale launch.

Complexity

As seen in many failed platforms, over-complicating the user experience serves as one of the most significant inhibitors to developing a successful social networking platform. Adoption and retention of any technology solution is largely dependent on simplicity and functionality. As such, the platform cannot attempt to be an end-all-be-all technology solution. It should be specific and exclusive to a particular type of social networking rather than a mash-up of different tools. For example, a Facebook-like platform that incorporates a Twitter-like feed, a YouTube-like video library and a LinkedIn-like profile design, has continuously proven to be ineffective.

Groups Feature

This is commonly provided as a security feature, so that users can only gain access to certain silos of information. However, this approach tends to cramp the growth and value of social networking. Even the most notable public social networking platforms continue to fail in doing this. The original Facebook "friends lists", which allowed users to categorize their friends into groups, was used by less than 5% of its users.¹⁴ Today, even as Facebook has revamped this "groups" feature to include a variety of new benefits, it continues to attract criticism. Sort of like creating a new file folder on your computer, most people usually start with creating a folder and then fill it up with documents before they begin to create sub-folders. The same should be done with a social networking platform. The option for a user to categorize his or her friends into groups should exist; it just shouldn’t be made available until the user-base is large enough for it to be needed.
Cost

The current economic climate and the declining budgets of most police organizations certainly provide a challenge to establishing a social networking platform for law enforcement. The danger however does not lie in spending money on implementing such an effort. If done correctly on the first try, the law enforcement and homeland security community will actually save a significant amount of money. But if the effort is not coordinated, the vendor is not fully evaluated, and/or the wrong platform is acquired, then it can certainly become cost prohibitive.

Acquisition

Moving forward to acquire the right solution should be seriously considered by the Major Cities Chiefs Association and the Major County Sheriffs Association. There is no question that establishing a national and secure social networking platform for law enforcement would prove very useful and likely transformational. The following are three options for advancing this effort:

Option 1 - Modified Version of Copbook

The Copbook technology appears to be a viable option for establishing an effective social networking platform for law enforcement. Having tested the Copbook software, several areas for improvement have been identified. If modified as proposed and with built-in flexibility, a post-pilot version of the Copbook software could prove to be an effective solution.

After revamping Copbook so that it would fit the specific needs identified in this report, each agency would agree to purchase the program separately and at an annual or monthly rate. Access to the program would cost a large-sized agency approximately $24,000 annually. This would include and be useful to every employee that belongs to that agency. For example, for the Las Vegas Metropolitan Police Department, all 4,000 of their employees would be granted access and more importantly, all of these employees would be able to find value in it.

The annual membership model would allow agencies to adopt the software on a tentative basis so that they could further evaluate its usefulness before permanently committing. If most agencies cannot afford to purchase the platform at this time, then the MCCA and MCSA should consider working with federal partners to help fund or subsidize this effort. There should also be some consideration towards merging the myHomeland effort, which DHS is currently piloting, with Copbook. This would help with funding and preventing duplication.

Option 2 - Pilot Additional Platforms

Another option would involve conducting additional pilot programs to determine whether other platforms possess the potential for establishing a social networking platform for law enforcement. While an out-of-the-box version of any of the pre-existing platforms would likely not work, customizing one of these solutions after a successful pilot could offer some potential.

Option 3 - Formalize and Acquire Support

The third option is to propose an MCCA and MCSA resolution for a formal vote, that supports establishing a social networking platform for law enforcement, and follow this with forming an executive task team to aggressively lead the effort. The resolution would help formalize the need and solidify the requirements that are outlined in this report. In turn, this will help attract support from partner agencies and it’ll motivate vendors to modify their platforms to fit our specific needs. The formation of an executive task team, which is just as important, would help acquire the needed funds through grants or other means; make a final determination on the best platform; and facilitate its implementation.
SPECIAL THANKS

This research would not have been possible if not for the many partners and participants that contributed throughout the process. In particular, a special thanks to the Major Cities Chiefs Association, the Major Cities Intelligence Commanders Group, the Major Counties Sheriffs Association, the Major Counties Intelligence Commanders Group, Copbook, the 167 Copbook Pilot Participants, and the 54 agencies that they represented. Also, if not for the leadership, forward-leaning perspective, and support of Sheriff Douglas Gillespie and Assistant Sheriff Greg McCurdy, this endeavor would not have been feasible.

EXECUTIVE SPONSERS

Sheriff Douglas Gillespie (LVMPD)  Assistant Sheriff Greg McCurdy (LVMPD)
Executive Director Darrel Stephens (MCCA)  Chief Art Acevedo (APD)
Sheriff Rich Stanek (MCSA)  Deputy Chief Michael Downing (LAPD)
Division Chief Paul Kissel (ODNI)  Deputy Chief James Owens (LVMPD)
Director Mike Sena (NFCA)  Assistant Chief Clark Kimerer (SPD)
Captain Andy Mills (SDPD)  Ret. Deputy Chief David Carter (HPD)
Commander Walter Smith (PPD)  Lieutenant Spencer Bakke (MCSA)
Ret. Deputy Chief Michael Grossman (LASD)

CONTRIBUTERS

Analyst Adam Walker (LVMPD)  Detective Jim Rewald (LASD)  Captain Harold Pretel (CDP)
Detective Jason Leavitt (LVMPD)  Lieutenant Donald Tuten (JSO)  Chief of Detectives Dennis Richards (BPD)
Officer Juan Zaccheus (APD)  Sergeant Jeff Rogers (APD)  Deputy Chief Albert Salinas (LVMPD)
Captain Steven Carter (DPD)  Analyst Nicholas Emerick (EPPD)  Captain David Azuelo (TPD)
Lieutenant Joseph Chacon (APD)  Detective Sergeant John Celentano (LAPD)  Captain Patrick Bryne (OCPD)
Analyst Majorie Israel (LAPD)  Captain John Stedman (LASD)  Detective Oscar Armenta (SDPD)

ABOUT THE AUTHOR

Dori Koren is a Sergeant with the Las Vegas Metropolitan Police Department and the national coordinator for the major cities and counties Criminal Intelligence Enterprise (CIE) initiative. His focus has included developing policies, projects, and processes regarding law enforcement’s use of social networking, violent extremism, homeland security, intelligence, and prevention. He has a B.A. from the University of Nevada, Las Vegas and he is currently coordinating the national effort of establishing a social networking environment for law enforcement, as well as the development of domain assessments and collection practices for major law enforcement agencies across the Nation.

For questions or more information regarding this report, please contact Sergeant Dori Koren at D9007K@lvmpd.com.
2. Avanade. (2013). Global Survey: Is enterprise social collaboration living up to its promise?