OFFICER®

THE LEADER IN PRODUCTS, TECHNOLOGY AND INNOVATION

SUMMER 2024

Exclusive Officer eHandbook on

TECHNOLOGY

ENDEAVOR BUSINESS MEDIA

CONTENTS

SUMMER 2024

OFFICER®

EXCLUSIVE ONLINE CONTENT OFFICER.COM

Police Transparency Through Technology
Can L.E. agencies data increase transparency and public trust?
Officer.com/55056775

Drones as First Responders
In recent years, law enforcement drones have become vital tools.
Officer.com/55089888

Exploring the World of Technology in L.E.

Paul Peluso is the Managing Editor of OFFICER Magazine and has been with the Officer Media Group since 2006. He began as an Associate Editor, writing and editing content for Officer.com. Previously, Paul worked as a reporter for several newspapers in the suburbs of Baltimore, MD.

If you have any comments or questions, you can contact him via email at paul@officer.com.

Technology affects almost every part of law enforcement. While this has been the case for some time, the technology used by officers and command staff has become more complex and layered in a short period of time, and it can be tough to keep up with the newest trends. To help address this problem, the Officer Media Group added Toni Rogers to supplement its technology coverage. Rogers is a former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Rogers now provides content marketing and writing through her company, Eclectic Pearls, LLC.

During her time with Officer Media Group, Rogers has provided a number of articles and resources to help readership gain a better understanding of what technology is currently available and how law enforcement agencies can leverage it. In this eHandbook, you will find a collection of her work that touches on multiple areas of technology in law enforcement. Some of the types of technology covered include Computer Aided Dispatch (CAD), Records Management Systems (RMS), artificial intelligence, video surveillance, gun detection software, drones, body-worn cameras and much more. Rogers does a great job at both informing the reader as well as making a good case for some of the strategies and policies that law enforcement agencies must have in place.

Thanks for taking the time to read our Technology eHandbook and keep an eye out for other eHandbooks the Officer Media Group plans to make available in the near future!

Take care,

Paul Peluso

OFFICER

ENDEAVOR BUSINESS MEDIA

PUBLISHED BY ENDEAVOR BUSINESS MEDIA, LLC
30 Burton Hills Blvd, Ste. 185, Nashville, TN 37215
Phone: (800) 547-7377

EDITORIAL

Editorial Director	Frank Borelli
Managing Editor	Paul Peluso
Associate Editor	Joe Vince
Contributing Editor	Lindsey Bertomen
Contributing Editor	William L. Harvey
Contributing Editor	Brendan Rodela
Contributing Editor	Toni Rogers

EDITORIAL ADVISORY BOARD

Chief William Harvey (ret)
Sgt. Richard Nance (ret)
Cpl. Ian Webster
Deputy Tom Perroni
Mrs. Laura Burgess
Mr. Jason Meyer

SALES

Vice President/Group Publisher	Bill MacRae | 732-804-1732
Associate Publisher	Tom Burr | 615-403-6802
List Rental	Elizabeth Jackson 847-492-1350 Ext. 18 ejackson@meritdirect.com

PRODUCTION

Production Manager	Patti Brown
Ad Services Manager	Shirley Gamboa
Art Director	Kermit Mulkins
Audience Development Mgr	Delicia Poole

ENDEAVOR BUSINESS MEDIA, LLC

Chief Executive Officer	Chris Ferrell
President	June Griffin
Chief Operations Officer	Patrick Rains
Chief Revenue Officer	Paul Andrews
Chief Digital Officer	Jacquie Niemiec
Chief Administrative/Legal Officer	Tracy Kane
EVP/City Services	Kylie Hirko
EVP/Endeavor Business Intelligence	Paul Mattioli
VP Accounting	Angela Mitchell
VP Business Development	Paul Andrews
VP Content	Travis Hessman
VP Customer Marketing	Angie Gates
VP Digital & Data Innovation	Ryan Malec
VP Digital Ad Operations	Teresa Gebler
VP Finance	Jessica Klug
VP Production Operations	Curt Pordes
VP Sales Operations	Missy Zingsheim
VP Technology	Glenn Scheithauer

SUBSCRIPTION CUSTOMER SERVICE
(877) 382-9187; (847) 559-7598; fax (800) 543-5055
e-mail: officer@omeda.com

ARTICLE REPRINTS
e-mail: reprints@endeavorb2b.com

LIST RENTAL | INFOGROUP
Michael Costantino | (402) 836-6266
Michael.Costantino@infogroup.com
Kevin Collopy | (402) 836-6265
Kevin.Collopy@infogroup.com

OFFICER (USPS Permit 016-830, ISSN 2766-2926 print, ISSN 2766-2934 online) is published six times annually in Jan/Feb, Mar/Apr, May/Jun, Jul/Aug, Sept/Oct and Nov/Dec. by Endeavor Business Media, LLC. 201 N Main St 5th Floor, Fort Atkinson, WI 53538. Periodicals postage paid at Fort Atkinson, WI, and additional mailing offices. POSTMASTER: Send address changes to Officer, PO Box 3257, Northbrook, IL 60065-3257. **Subscriptions:** Publisher reserves the right to reject non-qualified subscriptions. Subscription prices: U.S. $58.75 per year; Canada/Mexico $86.25 per year; All other countries $126.25 per year. All subscriptions are payable in U.S. funds. Send subscription inquiries to Officer, PO Box 3257, Northbrook, IL 60065-3257. Customer service can be reached toll-free at 877-382-9187 or at officer@omeda.com for magazine subscription assistance or questions.

What's the chatter all about?

OFFICER™ ROLLCALL

OFFICER Magazine's podcast series covers subjects of interest in law enforcement. Our editorial team, along with industry experts, fill each podcast episode with information that is of value to law enforcement professionals and entertaining for all listeners.

SUBSCRIBE WHEREVER YOU LISTEN TO PODCASTS

officer-rollcall.podbean.com

Informed Policing Through Technology

Increased data-sharing, data gathering, and improved algorithms could combine even more data to support what many police officers already knew about their area and could even provide a new perspective.

By Toni Rogers

The improvements in computing capabilities and the availability of sharing large amounts of data provide real-time enhancements in policing. Shared data through CAD-to-CAD systems, the ability to query neighboring agencies' records management systems, using algorithms to find geographic and other crime patterns and artificial intelligence reviewing material while creating transcripts and finding anomalies are all instances of using updated technology to improve policing.

Officers have long known where the hotspots for types of crime are within their jurisdiction. Increased data-sharing, data gathering, and improved algorithms could combine even more data to support what many police officers already knew about their area and could even provide a new perspective.

Artificial Intelligence

The improvements in AI allow software to process large amounts of data to find commonalities, patterns, similarities, and trends. Combing through hundreds of reports, license plate reader data, and querying or calling other agencies can take several staff hours. With artificial intelligence (AI), the data can be reviewed much more quickly, and the information can be extrapolated for review.

Some of the current programs using AI and updated algorithms continue to provide options for law enforcement - options like the ones below that can save staff time while improving public safety through technology.

- **Video surveillance** – systems that provide facial recognition, biometrics, smart cameras that follow motion, aerial surveillance drones, and high-quality video that AI can monitor in real-time and warn of impending threats or flag suspicious video for timely review.
- **Locational data** – real-time crime mapping and gunshot detection software collect information and review it quickly to determine the locations officers need to focus on. Technology is also improving and becoming more adept in detecting growing crowds so officers can be updated proactively.
- **Field data** – including body-worn camera footage, real-time reporting and updating of the call through the computer-aided dispatch (CAD) system, and reports filed from the field. With CAD-to-CAD sharing, the jurisdictional borders that bad guys may cross are also open for artificial intelligence to query and consider as part of the analysis.
- **Training** – Review of body camera footage by a program designed to review every frame of video for behavioral concerns and create a transcript of the incident frees up supervisory time needed to spot-review the footage. The flagged video does not indicate wrongdoing, but it can save staff time while reviewing all the footage and flagging anything of concern for further review. Quality assurance of dispatch recordings can also provide the same review through AI, listening to the calls and looking for any flags that require more review.

Forecasting

The often-overused phrase, data-driven policing, encompasses the use of data, with more data being better, to make informed decisions on policing. Much like the phrase predictive policing that sought proactive policing through data analysis in the mid-2000s, both seek to use data to make the best use of available staff and resources while seeking to deal with crime proactively. The proactive part of policing is the most difficult aspect and technology is helping law enforcement make those decisions.

The increased points of data available allow AI to determine hotspots for criminal activity and even narrow down suspects based on data mining. One of the considerations with using existing data is knowing there may be biases included in the data. Much like forecasting the weather uses historical data and includes scientific analysis of current conditions to predict upcoming weather concerns, predictive policing or data-driven policing seeks to prepare today for what may happen tomorrow. As with forecasting the weather, policing needs to use outside sources and other evidence as a guide to the final decision.

As with forecasting the weather, policing needs to use outside sources and other evidence as a guide to the final decision.

The future through technology

The future of policing relies on technology. A recent study determined that AI technologies could reduce crime in a city by 30 to 40 percent. As artificial intelligence improves and data-sharing between systems within the same agency and the systems of other agencies becomes commonplace, law enforcement may be able to predict crime and crime hotspots more accurately.

As we begin to embrace technology fully and AI finds its footing in policing, not only do we need to heed changing legal circumstances surrounding privacy laws and similar cyber mandates, but we need to share that data with other law enforcement agencies. Criminals do not seem to mind crossing jurisdictional boundaries, and police data should also cross those geographic lines to keep the public and responders safe.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

Mitigating Technology Risk Through Planning

ID 122741723 © Alexandersikov | Dreamstime.com

Risk management allows a law enforcement agency to evaluate risks and forecast where things might not work as expected. **By Toni Rogers**

Risk is inherent in every aspect of law enforcement, and technology is no different. As more agencies rely on technology, there will be problems: system failures, lines down, power disruption, or something to interrupt your agency's technology.

In early 2024, AT&T's commercial wireless unplanned network outage resulted in no service for thousands of AT&T customers. This outage minimally impacted some police agencies but serves to remind us commercial network outages have happened before and will happen again. And most importantly, this recent outage serves as a reminder to have a plan when technology fails.

Managing risks

Risk management allows an agency to evaluate risks and forecast where things may not work as expected. Forecasting should be done with agency technology, including software, hardware, networks, and connections. The plan for managing those risks should include backup plans for the continuity of critical services for each staff function.

Some of this may be part of the agency's disaster recovery planning, but the plans for staff need to be more detailed and specific to each part of the technology. Procedures need to be in place for staff to know how to handle calls for service, records requests, 9-1-1 calls, arrest

and booking, and other routine tasks during system, power, and other outages. Police departments rely on technology, and knowing how to continue public safety services during system downtime is critical.

Redundancy

System redundancy and having a backup plan are critical for law enforcement technology. In the case of a commercial network outage, like the recent outage where thousands of AT&T cell phones were down in some areas along with Internet connectivity, an agency might consider having a redundant technology provider or a way to exchange data between the Computer Aided Dispatch (CAD) and Records Management System (RMS), and the patrol unit computers.

With all the pieces of technology in place as part of law enforcement, each point of failure must be considered and a backup option chosen, if possible. If there is no backup option, staff needs to know the workaround solution to continue providing public safety during technology downtime.

Communication plan

On-duty staff must know who to contact when a system does not work as expected. At some point after the initial assessment, communicating the outage to the proper government leaders and the community should be considered, and the plan will outline who communicates the information and what channels are used for community notifications.

Knowing when to notify the media of downtime and having a plan allows those decisions to be made before the situation. The plan also provides the notification's basics and establishes preset plans to share with the community. A plan of action for system downtime, especially when public services are disrupted, helps the agency keep the community informed, involved, and safe.

Training for system outages

System downtime is difficult to manage when scheduled but more challenging when unplanned. Staff should know what protocols to follow depending on the system that is down and where to get any needed supplies. For example, if the CAD system goes down, the telecommunicators need to know how to track service calls without CAD. Patrol units must know the protocol for running information searches if their mobile data computers are down.

Law enforcement uses many types of technology, and most know how to go back to "old school" ways when systems are down. As employees retire and leave their positions, knowledge of how to do things before technology can be lost. With a plan in place and training in case of technology failures, agencies can manage system or network downtime much more safely and effectively.

Restoring systems

Each piece of the system, such as a network component, software program, or hardware piece, is only part of a larger chain comprising the agency's technology. When part of the chain is out of service, bringing the rest of the technology back up to speed needs to be done following the proper protocol. Including those startup procedures in the plan can help staff bring back systems in the correct order to avoid complications or other problems that lead to additional downtime.

Even if your agency has technology staff or vendors that have responded to assist with the start-up process to ensure equipment health, agency staff will also have specific restart procedures for their work area. As with the example of the down CAD system, staff needs to know how to back-enter data as the system comes back online without losing required information like call times, responding officers, times on scene, and more.

Preparation and planning

Technology downtime is inevitable. Preparing for various technology outages—planned and unplanned, commercial and private—helps the agency weather the downtime and quickly return to normal operations. If your agency does not review technology regularly, consider adding the technology systems to an existing equipment review that includes repair, refresh, and replacement plans. The plan for technology downtime should also be revisited and reviewed when new technology components are added, replaced, or upgraded.

The benefits of planning and including staff training on the appropriate responses during outages can help mitigate the risk to your agency during technology downtime. A plan to handle technology downtime can minimize the impact on the community and provide alternative solutions to keep patrol officers and residents safe.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

Building a Sustainable Technology Budget in Law Enforcement

By Toni Rogers

Technology, networks, systems, big data, cybersecurity, and more are commonplace in police agencies and now take a large portion of each department's annual budget. Each technology piece used to manage the data has a yearly maintenance cost. Network equipment has annual service contracts to ensure the agency stays online and connected to the various systems and programs. Software, applications, and program upgrades must be included with annual maintenance or budgeted separately. Hardware and equipment will need repair or replacement, which must be considered in the budget.

Tracking the annual costs of each piece of technology and their increases must be part of technology planning and purchasing. Each new program or resource that may save staff time may be beneficial initially, but what about the long-term costs? Can the agency's budget absorb the annual maintenance, upgrade, and service fees after the initial deployment? Is there a trade-off cost that must be made, and if so, is the trade worthwhile to the community and the agency?

Reallocating resources

Some departments are working with staffing numbers far below the total number of authorized staff for that agency. Some of the push to take funding from police agencies has lessened, yet agencies like Cleveland Police are seeing city leaders ask for fewer officers as officer positions remain unfilled. Even with the decreased number of officers in Cleveland's proposed budget, the overall budget for the police department is higher based on staff raises and increased starting officer pay. The Cleveland mayor's proposed budget includes sustaining efforts using a "data-driven approach to solving crime," including the previous year's budgeted civilian crime analyst positions to manage the data.

The agency must continually look at its technology plan and associated budgeting needs.

This asks the question, should policing focus be placed on technology? Traditionally, police department budgets have a more significant part of their budget for salaries. As agencies reduce officer numbers based on unfilled positions and lean more heavily on technology, how does the overall agency change? And is that change a welcome one in the community?

Technology should be a tool to assist in lowering response time and meeting other agency mandates and goals. Technology can be leveraged to save staff time, help keep officers and the community safe, improve response times and investigation success rates, and so much more. However, reallocating resources to technology from units with excess budget due to open staff positions should not be done lightly. Moving budgetary resources away from staff should include a workload analysis to determine if lowering the staff levels will negatively impact the short-term and long-term goals of the agency, like response times or proactive policing.

Effective planning

Planning for technology upgrades, equipment replacement, and purchasing new programs or applications is not a one-and-done endeavor. The one-time cost may include first-year or even second-year maintenance fees, but knowing what is included and when the ancillary contract costs are due is critical to effective planning and budgeting. Those added maintenance and upkeep annual fees increase as technology stacks up. This hit to the budget can be quite a shock. Technology purchased through grants has to be included as well. Even without the initial budget 'hit' for implementation and deployment, the recurring fees, upgrades, and replacements for technology purchased through grants eventually must be absorbed into the budget.

Agencies often focus on using technology to improve officer safety and better use of patrol time by removing tedious tasks like data entry. In a workforce assessment, these technology-based improvements might show a slight need for decreased staffing. Conversely, the workforce assessment may also show additional staffing needed to manage the network, programs, and equipment. Justification for new technology should always consider the long-term impact on staffing, systems and equipment, internal processes, and, most importantly, annual maintenance and upkeep fees.

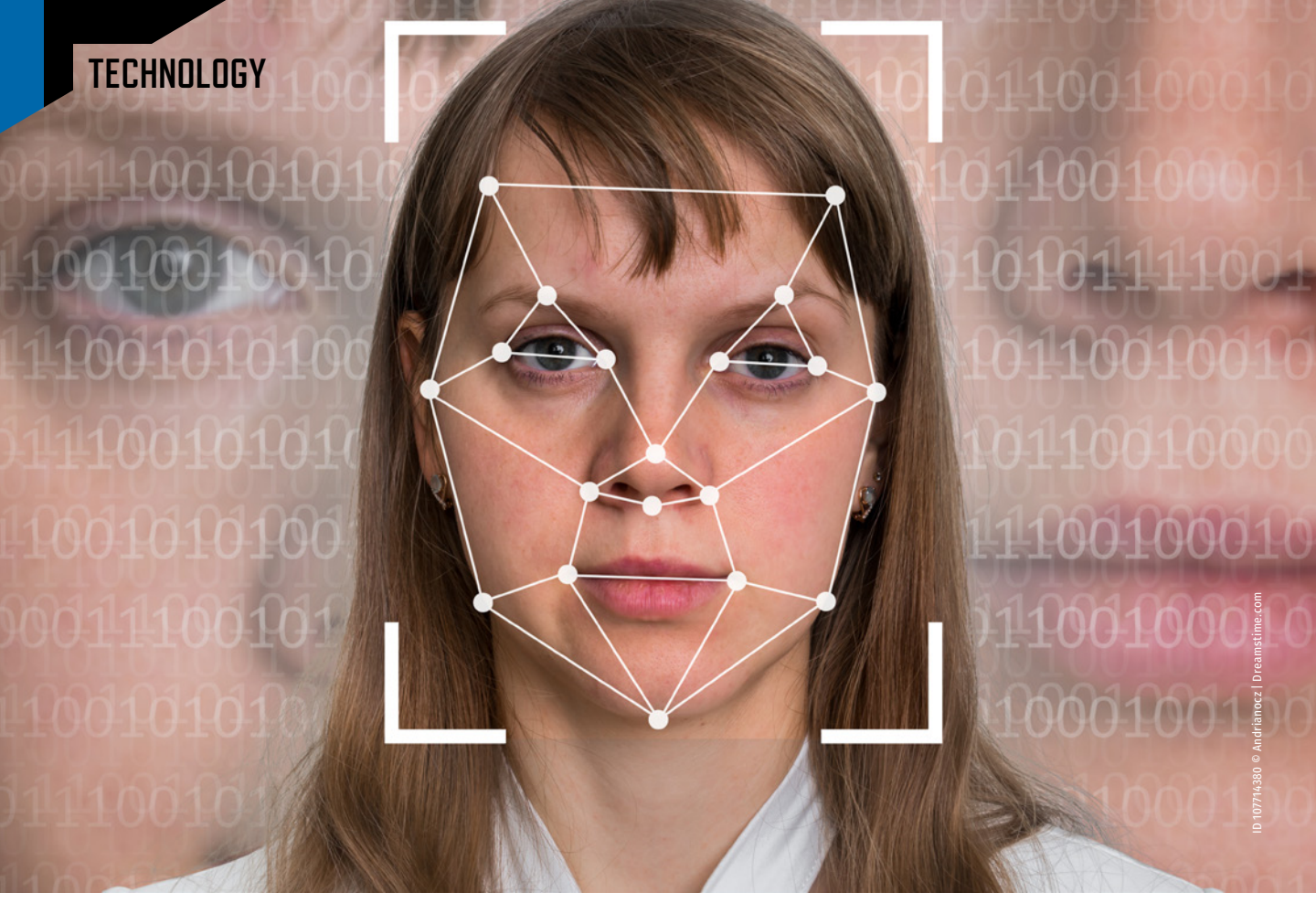
Technology plan

A technology plan may be part of an agency's capital improvement or 10-year department plan. If not, each agency should have a goal of at least five years, including technology, anticipated budget, staff, and service levels. The long-range plan needs to be reviewed frequently, including the current technology, the planned technology, and the agency's future wish list. All known and anticipated budget numbers need to be included in this long-range planning. Including current budgeting maintenance numbers may require decisions on future technology implementation based on future economies and budgets.

Technology planning must consider the current situation and how everything associated with the latest program, application, or equipment fits in the long term. Technology changes rapidly, making updates, upgrades, and new equipment needed regularly. The agency must continually look at its technology plan and associated budgeting needs. The known and anticipated technology, physical footprint, staff needs, costs, and recurring fees must be included in the budget, building and space, staffing, capital, and partnership plans.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.



Using Facial Recognition Technology in L.E.

The increased use of technology, like facial recognition, puts law enforcement in the crosshairs of many. **By Toni Rogers**

Law enforcement often balances public safety and individual privacy with technology. The increased use of technology, like facial recognition, puts police in the crosshairs of politicians, the media, and community transparency groups. Law enforcement must use current technology to keep up with criminals who willingly embrace new technologies.

As with any investigatory strategy, facial recognition is not the definitive answer to solving the case. However, the technology can and should be used by law enforcement agencies to generate leads. Oftentimes, a good lead is all that an investigator needs in order to solve a case.

▲ Facial recognition is a strong forensic tool, but also a contentious privacy issue.

What is facial recognition?

Facial recognition uses machine learning algorithms (where the machine learns what to do from matches and how to improve searches through incorrect results) to look for matches to a photo from within a set database. The search uses data points in the image to find matches. Poor lighting of the image being searched, the addition of glasses, a face mask, a hat, or other items can impede system recognition. Shadowing or a side angle of the face, rather than a front view, can also negatively impact a match. Facial recognition is also affected by human aging; changes in facial features from weight gain or loss or cosmetic surgery can also challenge facial recognition.

Law enforcement most frequently uses facial recognition through vendor software that is available commercially. The vendor holds the images, often pulled from social media, and uses those images and their associated data points to search through during a query by law enforcement. More recently, some policing agencies have started using software applications to search private databases, like driver's licenses and booking photos.

Security and policing uses of facial recognition

Facial recognition technology has grown exponentially in the last several years. Before 2018, Federal law enforcement used facial recognition sparingly. A GAO report found that, as of 2023, seven law enforcement agencies in the Department of Homeland Security and Department of Justice use commercial and nonprofit facial recognition services.

The GAO report did not consider the Transportation Security Administration (TSA), yet TSA has tested facial recognition in several situations. Harry Reid International Airport in Las Vegas, Nevada, recently introduced passenger self-screening security lanes. These lanes demonstrate the abilities of current technology in security screening, which includes using video analytics as part of the "Screening at Speed" program to verify passenger identity.

Current applications

- In January 2024, an arrest was made in the January 2021 capitol incident using facial recognition. The suspect was located by matching incident photos to social media posts from a personal Facebook account, which led to the arrest.
- A news report out of Colorado states that police agencies, both local and federal, are using the Colorado DMV facial recognition program to find investigative leads. The report found that the use of DMV photos for facial recognition by law enforcement started at 42 uses in fiscal year 2012-2020 and was up to 157 uses last fiscal year. The news report also pointed out that using facial recognition is only to obtain possible leads, not probable cause for arrest, nor is it enough to get a search warrant.
- Some international agencies also use facial recognition to prevent and prosecute retail theft. The same facial recognition software, available commercially, is also being used by some stores in the UK to prevent future theft. In the U.S., the NYC mayor has encouraged retail stores to employ facial recognition to deter and prosecute shoplifting and theft. In a different use case, Madison Square Garden uses facial recognition scanning through a vendor to identify attorneys in litigation with the venue.

Privacy and political concerns

Last week, the Government Accountability Office (GAO) released an update on facial recognition, reiterating the need for staff training and other recommendations for agencies using facial recognition. In addition to training requirements, the GAO recommends addressing privacy requirements and concerns and implementing policies on facial recognition to aid in transparency and acknowledge civil rights concerns. The Bureau of Justice Assistance released a policy template in 2017 specifically for facial recognition use in intelligence and investigative actions. That template includes addressing privacy concerns in the agency's policy.

Politicians, especially in election years, often look at technologies that may seem invasive to some citizens. Some states have weighed in on law enforcement's use of facial recognition, and there are laws, such as the one in Colorado, stating that the results of a facial recognition search may only be used as an investigative lead. Now, Congress is looking at federal agencies' use of facial recognition. Whether additional laws will be enacted governing the use of facial recognition is unknown; each agency using this technology should know the laws that impact their searches.

Identifying suspects

Facial recognition technology continues to improve, and case law and new laws are being enacted to influence how law enforcement uses this tool. Facial recognition can help investigators obtain a lead more quickly in certain situations. Just as policing has relied on eyewitness identification of suspects, facial recognition through machine learning offers the same.

In today's world, surveillance is expected. Many public jurisdictions, private companies, and even private households have cameras that record activity. Facial recognition technology will only continue to improve through continued use. With more photos to search being added to databases regularly, the ability to find possible matches continues to improve. Law enforcement will continue embracing technology tools like facial recognition to bolster existing investigation processes. Agencies that lean on these tools to augment staff efforts should also include policies and training to help protect not only the agency but also their staff and provide transparency to the community.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

The Importance of Redundancy in Law Enforcement Technology

Having a plan B is essential when it comes to public safety technology. **By Toni Rogers**

The recent 9-1-1 outage in several states caused by a fiber cut during the installation of a light pole highlights the system's fragility and stresses the crucial need for redundancy in public safety. The most recent outage impacted Nevada, South Dakota, and Nebraska for approximately three hours, impacting the public's ability to reach 9-1-1. Areas with text-to-9-1-1 capabilities urged residents to text 9-1-1 or use a landline to call 9-1-1.

A separate incident occurred at the same time in the area of Del Rio, Texas, and impacted residents' abilities to reach 9-1-1 through a specific cellular carrier. Residents were told to use another cellular carrier or a landline to reach 9-1-1. These two incidents, which occurred on the same date and at similar times, highlight the need for redundancy in public safety systems and stress the importance of having a plan to deal with outages.

Plan B

A plan B or a backup plan is second nature in law enforcement. Police officers are trained to know what to do in case different scenarios happen on the scene. They are also trained to adjust and think on the fly when situations change. The same training, thought, and planning need to be in place with public safety technology and the staff that works with the systems.

Sometimes, the system failure is minimal and easy to fix, such as a non-functional body-worn camera that is exchanged for an operational one. Sometimes, the outages, like Computer-Aided Dispatcher (CAD) or phone system downtime, can be more large-scale. Having procedures that are known to staff helps maintain officer safety, community safety, and the integrity of case-related evidence.

ID 112151383 © Blurf | Dreamstime.com

Redundancy planning

Frequent technology improvements and updates help law enforcement agencies do their jobs more effectively. Agencies rely on these technology pieces, so planning a redundant path to avoid failure is critical. Public safety agencies rely on electricity or other forms of energy to keep the numerous technology pieces operational. When the power goes out, most agencies have a backup generator that turns on to power their systems. That generator should have regular maintenance and test runs to ensure it will function as intended when needed.

Planning redundancy for the facility is only part of the overall technology used in law enforcement. Systems often integrate or connect through a shared network or even have hardware in the same room. An air conditioner not working to control the server room temperatures can take down several vital systems. The shared network can leave an opening for hackers to access and damage critical systems. The connection to the Internet could go down, leaving some systems only partially functioning. Downtime does not always indicate a system failure or power outage. Working through the possible downtime scenarios to create a response plan and procedures to follow for those events lets the agency operate at even basic service levels.

Training for the future

Law enforcement is used to contingency planning and continuing to provide service even when equipment fails, staffing is low, and systems are down. As much as training programs focus on using the technology and equipment that are part of policing, training staff on how to work around and without that technology and even some equipment will help minimize the stress of the inevitable system and equipment failures. With a plan in place, the staff knows how to deal with downtime or equipment failure and what protocols to follow for command, community, and media notification.

Much of the world relies on technology daily. As much as we rely on it, we're also not surprised by downtime—inconvenienced, but not surprised. Law enforcement is no different. Sometimes, reverting to 'old school' ways of writing down call information may not work as quickly as we'd like, but when the technology fails, emergency calls don't stop or wait until things are back up and running.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

How Technology Can Help L.E. Officers Manage Mental Health

Wearable sensor technology can help police and law enforcement officers track their physical and mental health.

By Toni Rogers

Police officers are not strangers to mental health—both from answering calls for service and from their own traumatic experiences on the job. During Mental Health Awareness Month in May, there were many public service campaigns attempting to stem suicides and to work on bringing awareness of checking in on your mental health and the mental health of those around you.

According to a report by CNA Corporation, an analysis of information on law enforcement officers' mental health showed officers experienced suicidal ideation at approximately twice the rate of the general population. With the increased access to artificial intelligence and machine learning, agencies should consider using technology to help track and mitigate stress, trauma exposure, and other mental health concerns in law enforcement officers.

What the numbers say

Larger agencies with more than 100 full-time sworn officers represent the majority of law enforcement deaths by suicide. These agencies encompass nearly 11% of all law enforcement agencies nationwide, yet public safety deaths by suicide for this group of agencies is 61%. Significantly, 68% of deaths by suicide occur at the officer rank, 21% held mid-management roles, and approximately 7% were investigators.

Currently, serving law enforcement personnel accounted for 72% of deaths, according to the report. Can using technology and associated applications help officers through issues with their mental health? Some recent improvements in wearable technology and machine learning show promise in tracking officer mental health and overall well-being.

How technology can help

Many commercial wearable sensor technology (WST) devices are available to track activity level, time spent on the activity, and heart rate. WST advancements continue to improve and could prove beneficial in tracking officer health and safety. A study conducted through the Police Executive Research Forum (PERF) on behalf of the National Institute of Justice (NIJ) found that commercially available WSTs are not yet accurate enough to inform decision-making in a law enforcement environment.

While they may not drive decision-making in the field, WSTs can help officers track their physical and mental health. Monitoring heart rate during times of low stress versus times of high stress after a call can provide insights into stress management. Tracking sleep between shifts and monitoring associated sleep patterns can also provide clues to mental health. Checking heart rates after overtime shifts or shifts with little sleep in between could signal health concerns that can be handled before they escalate. WSTs can also track sleep and remind the wearer to exercise, drink water, or engage in other healthy activities.

Using the Data

With tracking comes data and data analysis. Capturing data also allows sharing that data with other systems, such as training simulators. The biometric data collected could help officers learn to control their stress levels through practice. Minimizing stress can help cardiovascular and mental health, weight gain, and sleep while having other positive impacts. The WSTs would also save the biometric information for later review to help provide training feedback.

Unlike calls for service or investigation data, information from the WSTs would include an individual's health information, such as heart rate, weight, sleep patterns, exercise, food consumption, and more. Similar health-related apps that many people have on their smartphones share that data anonymously with the app company, and most users agree to share the data to use the app. With data gathered and analyzed by a law enforcement agency, there are concerns about who can access this data and what privacy rules should be determined before implementing this data collection.

While they may not drive decision-making in the field, WSTs can help officers track their physical and mental health.

Tools for self-care

Several factors contribute to law enforcement officer's mental health. With changing schedules, different sleep patterns, trauma witnessed on the job, and the stigma attached to seeking help, those who work in public safety need to safeguard their health—both physical and mental. Currently available technology, like WSTs and mobile apps, can help track health-related metrics and provide reminders. Subtle pushes from the app or WST toward healthier behaviors can lead to habit changes over time.

Managing the dangers linked to mental health through stress and trauma can be challenging. Healthy habits like maintaining work/life balance, devoting time to rest and relaxation, journaling, finding time to be with friends away from the job, and participating in hobbies can help alleviate stress and improve resiliency. And technology can play an essential part in helping law enforcement staff manage and improve their mental health.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

Technology in Smaller L.E. Agencies

When it comes to implementing technology, smaller law enforcement agencies can and should leverage their unique abilities. **By Toni Rogers**

Each law enforcement agency has different technology needs. Some communities may benefit from a drone program, and others might benefit more from body-worn cameras or an investigations database. When it comes to implementing technology, smaller agencies can and should leverage their unique abilities as smaller departments to modernize and upgrade technology to fit their needs.

Managing technology upgrades and installations requires foresight, planning, scheduling, and so much more. Large agencies may have project managers to monitor and assist significant technology growth, but smaller agencies may have staff that are masters of many things. It is not uncommon to find a dispatcher or patrol officer in charge of one of the agency's tech systems. By embracing their way of implementing technology that best serves the agency and the community, a smaller agency can integrate the most beneficial technology.

Small agencies are the majority

Agency-wide technology requires planning from the purchase through the implementation and cutover. The agency's size plays a significant factor in determining the technology needed. In 2018, the number of agencies with fewer than ten full-time equivalent (FTE) sworn officers was 7,055, or approximately 40% of all state and local law enforcement agencies in the United States. The same 2018 data show that agencies under 100 FTE officers make up approximately 92% of the agencies in the U.S., and those with over 1,000 FTE sworn officers accounted for less than 1% of the agencies overall in the U.S.

Smaller law enforcement agencies have many of the exact needs of larger agencies. Still, they may lack the technology staff to implement programs and install equipment, often relying on vendors or third-party consultants. Their size allows smaller agencies to transition to new technology more quickly. There are fewer layers through the approvals needed for large projects, even without a large staff dedicated to the project.

Small agency benefits

At first blush, the larger agencies may have more access to technology upgrades or new installations. The needs may differ, but small agencies still want and need technology. And their small size may help them realize the benefits of technology more quickly than their larger counterparts.

Scale and complexity of operations

Agencies with lower staff numbers and restrictions must be creative when choosing and planning technology. Smaller agencies can also quickly purchase, implement, and test technology. These agencies typically operate within a more confined geographical area and handle fewer incidents than their larger counterparts. As a result, they may opt for simpler, more streamlined technology solutions that cater to their specific needs without unnecessary complexity.

Budgeting considerations

Smaller law enforcement agencies may need fewer technology systems than larger neighboring agencies. For example, smaller agencies have fewer specialty units than larger agencies, reducing the need for technology related to those units and letting the smaller agency focus on the technology that helps the agency provide policing in the community. Departments with fewer sworn officers can benefit from modernizing policing through technology, such as using drones to search an area or artificial intelligence to answer administrative phone lines. The key is using technology where the agency will benefit most.

Training and support infrastructure

Smaller agencies may need more resources to provide comprehensive training and support for technology adoption. However, they can leverage partnerships with vendors, government agencies, and regional training centers to access training opportunities and technical support. Sometimes, the agency may have staff members who are more adept at technology and can train others, including new hires, after the initial training period. This also happens in larger agencies, but the smaller agencies have fewer staff, making the training process faster.

Data management and analysis

Smaller agencies may have a different volume of data to manage than larger agencies, but every policing agency can benefit from adopting data management and analytics solutions. These tools help identify patterns, trends, and potential threats within their communities, enabling more targeted and effective law enforcement strategies.

Interoperability

Smaller agencies look to interoperability when budgetary or other constraints limit their ability to implement needed technology. Not only is cost-sharing a benefit, but the shared data and resources can help a small department stay updated with the technology required to manage employee retention and keep their community safe.

The future of policing relies on technology

Large and small law enforcement agencies recognize the importance of technology in modern policing. While large agencies may have more resources and infrastructure to support their technological initiatives, smaller agencies can still leverage technology to enhance their capabilities within their unique operational constraints.

The many changes in law enforcement technology can leave smaller agencies feeling behind. Leveraging the skills of the staff, the needs of the community, the types of data and analytics required of the technology, and budgetary constraints allow small agencies to be adaptable during technology upgrades and installations—something that will continue to be needed with the ever-changing technology landscape.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

ID 131912964 © Yanawut Suntornkij | Dreamstime.com

5 Considerations for L.E. Tech Planning

Understanding the plan and existing technology and knowing how the systems work together within the network allows new applications to become part of the solution. **By Toni Rogers**

Starting a new calendar year is a great time to look at your current technology and existing plans for technology growth. Many law enforcement purchases are considered technology, from large-scale projects like two-way radio systems, computer-aided dispatch applications, and digital evidence storage systems to body-worn cameras, license plate readers, and drones. Understanding the plan and the existing technology and knowing how the systems work together within the network allows new applications to become part of the solution. A solution that works best for the agency, the users, and the community.

Begin with a look at the strategic plan to see if your agency is on track or if some items need more focus. Then, review the technology items implemented over the last 12 months and determine if it is working as hoped, if the training was adequate, and if your agency is utilizing the technology to its fullest potential. The community may view agencies that use technology effectively as more transparent. The agency can also be more attractive to potential employees and retention of existing employees.

Assessing what you have

The first step is listing your technology, what works, and what is not being used. Include the appropriate staff with knowledge of hardware, network, systems, and software. For the technology lists, look at what percentage of your application is used and if any parts are not being used. This is the current big picture to see if technology is in place, what is upcoming, and what is in the agency's plan. The planning review should also point out any problems with existing systems, such as the duplication of data entry or other aspects that make it unpopular or ineffective.

Cybersecurity and maintenance

This is also an excellent time to check your network status, capability, and hardware. Is your agency using a schedule for upgrades, system patches, and upkeep? Who is responsible for the maintenance and verification of service? What about regular data backups and data storage? Verify the backups and storage capacity. The assessment should also include checking for security updates, outstanding system upgrades, or warranty extensions that may be needed.

Short-term planning

Any form of planning should include checking the budget. If your agency is mid-year fiscally at the new calendar year, are you at the halfway point of your budget for technology? Are there projects in capital expenditures for the year, and if so, are you on track to complete those projects? This is also a good time to check training records for existing and new technology and verify your hardware, systems, and software maintenance. The review is also a chance to determine if more training is needed on some of the software or if an aspect of the technology is no longer required or should be used differently.

Long-term planning

The next part of the review encompasses the assessment, the cybersecurity and maintenance, and the short-term plan. Take the information learned and determine what upgrades or maintenance may have been overlooked. Look for holes or missing applications that would improve one or more aspects of policing in the community. Are those applications on the long-term plan? If not, should they be added? Consider what technology the neighboring agencies are using and determine if there is an ability to share data or training. Determine if mutual aid agreements, inter-governmental agreements, and other formal (or informal) relationships may benefit from or be hindered by technology decisions.

The next best thing

Keeping an eye on the technology changes through conference attendance, reading updated product reports, and talking to law enforcement equipment vendors can inform your agency of the new technology. Meeting with other agencies also provides ideas and insight into the technology they have, including what works and how they use it. Speaking to staff and those who use the systems and applications will also determine what works and what they don't use and may even show some potential training gaps or needed policy updates. All of these should be considered when reviewing possible technology additions.

Technology is the future

Decisions to add new technology need a deep dive into the pros and cons, including the risks and benefits to the agency. Stanford University Law developed a toolkit to determine if emerging technology benefits a department. The toolkit has some great questions to consider when looking to add a new technology component. The responses could also help develop answers beneficial in budget presentations and grant applications. And with the assessments in place, when the new technology sounds like a good fit, it becomes easier to determine the best timeframe within the existing long-term plan.

The future is now

Law enforcement will always need the next great technology. And technology does amazing things that help agencies perform their duties. Not all new technology will benefit each law enforcement agency. Regular technology plan reviews allow your agency to assess whether the new technology fits. Like some field inspections, a technology assessment should be completed annually, with bi-annual reviews, to ensure the agency is on track for the year.

Technology is quickly becoming one of the mainstays in every part of the world, and law enforcement is no exception. Without long-term planning to include maintenance and upkeep, upgrades to ensure reliability and growth, and planning for integrating new software and hardware to serve your needs and those of your community, your agency may struggle to stay current. Each agency's technology needs will differ, but each department needs technology to increase safety, solve crimes, provide transparency, and manage employee recruitment and retention.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

The Importance of Data Sharing

Integrating data between different systems in a law enforcement agency can improve decision-making, collaboration, productivity, management and planning.

By Toni Rogers

Agencies frequently share criminals who move between geographic boundaries with ease. But sharing data is not quite as easy. Law enforcement databases are often siloed within their agency, with different data entry and database management policies that can make data sharing more difficult. Integrating data from separate systems within the same agency is vital, as data sharing between law enforcement agencies is critical in policing.

Rapid technological changes have increased the number of systems public safety staff must navigate daily during their duties. Management of and policies for data storage, security, retention, and data entry, must be revisited frequently as technology and threats to security evolve. But rather than viewing a large amount of data as cumbersome, integrating data between different systems in the agency can improve decision-making, collaboration, productivity, management, and planning.

Using data to support decision-making

Law enforcement has long used data to support decisions in administration and investigation. Even in the days of paper reports and logs, recorded details were necessary to solve cases and make the best staffing decisions. Technology today provides a broader view of the data and can integrate the numbers and patterns and use information dashboards and geographic hotspots.

Incorporating artificial intelligence (AI) in facial recognition, license plate reader, and even 9-1-1 communications systems creates another layer of information that should provide a large, integrated database. However, some of this data must be accessed individually. Looking for a person of interest may mean checking several systems and then connecting all the information on that person into one investigative file. Add in other databases like various courts, jails, and neighboring law enforcement records, and that process may not be quick.

Collaboration, efficiency and productivity

One of the benefits of data collection and sharing include collaborating with other agencies to prosecute criminals. Sharing with other agencies can help inform local and regional training programs and provide safety bulletins more quickly between nearby agencies. Data sharing can also create partnerships to apply for grant funding or collaborate to integrate similar systems, such as CAD to CAD data sharing and similar applications.

Another benefit is an increase in efficiency and productivity. Imagine an application dashboard or report-gathering mechanism that pulls the specified data from different agency systems to quickly give users a customized look at the information they need. For field units, that may be configuring the CAD application and mapping to show only their assigned areas. For command staff, the dashboard may include daily statistics, historical analytics, staffing levels, service times, and current calls for service.

Operations management and planning

Data integration and sharing between systems can impact operational planning too. Scheduling staffing for planned events could use historical data from previous events to provide an overview of the units needed. Incorporating the information from a training management database would quickly provide a list of personnel with specialized training, should those skills be needed for the event. Adding in the availability of units based on the scheduling program, management can see how many personnel are available and what the staffing costs would be.

Data sharing is also used for planning to determine if staff numbers need to increase or be reallocated to different geographic areas. Historical analysis can also find increases in call types that may require more training and even policy updates. For example, data history may show increased calls for service dealing with mental health situations. That information could lead to updated training, policies, and even new programs or partnerships to improve response and safety.

Data, data, and more data

Policing is hard enough without having to search multiple databases for information. Criminals do not limit their law-breaking activity to only one jurisdiction. Yet the public expects police to use technology to quickly access information and solve crimes. That information may be housed in other agencies, courts, corrections, county, state, or Federal databases.

The same public also demands transparency from police and expects the timely release of information. Information that may be sensitive or involved in an investigation or the information may not belong to the agency. Police are continually held to higher standards and expected to use technology as expertly and efficiently as private companies, often without the same funding and opportunities.

Given the benefits of data sharing and system integration, law enforcement must be able to access their own data from each of their systems, even integrating those systems when possible, to bolster decision-making, increase collaboration, efficiency, and productivity, and improve operations management and planning. As technology evolves, data sharing from integrated systems and sharing data across jurisdictions will become more common in law enforcement, and learning to leverage the technology and subsequent data through integration and sharing will be needed not only to increase the safety of police and the community but to move law enforcement agencies forward.

ABOUT THE AUTHOR

Toni Rogers is a freelance writer and former manager of police support services, including communications, records, property and evidence, database and systems management, and building technology. She has a master's degree in Criminal Justice with certification in Law Enforcement Administration and a master's degree in Digital Audience Strategies. During her 18-year tenure in law enforcement, Toni was a certified Emergency Number Professional (ENP), earned a Law Enforcement Inspections and Auditing Certification, was certified as a Spillman Application Administrator (database and systems management for computer-aided dispatch and records management), and a certified communications training officer. Toni now provides content marketing and writing through her company, Eclectic Pearls, LLC.

OFFICER VIRTUAL ACADEMY

REGISTER FOR FREE

OFFICER Virtual Academy offers self-paced online training for Municipal, County and State law enforcement agencies, DOD, Homeland Security and other specialty units.

Leveraging our research insights, forum discussions and industry expertise, we identified the top trending topics and grouped them into the following channels:

- On The Street
- Training & Careers
- Investigation
- Tactical

Our NEW online portal includes:

- Top navigation broken out into channels and learning pods.
- Easy-to-access courses in a variety of formats from videos, educational sessions, and interactive courses.
- Completion certificate based on time spent or quiz scoring.
- Downloadable content for future reference materials.
- Ability for users to reach out to sponsors via website, email or phone.
- Single sign on for users to track their training path.

Sponsored by

ASP

SAFARILAND®

Brought to you by

OFFICER MEDIA GROUP

OFFICER.COM OFFICER

VirtualAcademy.Officer.com