

# The New York State Chief's Chronicle



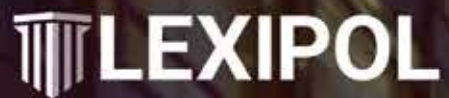
Serving New York's Police Executives Since 1901

March 2019



*Photo courtesy of the Buffalo News*

**In This Edition:**  
**Counsel's Corner**  
**Feature Article - Building Strong Community Relations**  
**FBI School Safety Initiative "The SRO Liaison Platform"**  
**The Puzzle Pieces of Cybersecurity**  
**Is Running Always the Best Option?**  
**Confronting Terrorism in New York State**  
**Technology Update**



# **BE CONFIDENT IN YOUR POLICIES**

Trust the only comprehensive  
public safety policy solution

- Continuously updated policies
- Scenario-based policy training
- Policy implementation assistance
- Web-based platform & mobile app

**SCHEDULE YOUR FREE DEMO TODAY**

844-312-9500

[info.lexipol.com/nysacop](http://info.lexipol.com/nysacop)



# contents

VOLUME 7 • ISSUE 1 • SPRING 2019



## In this issue

- 2 ON THE COVER**
- 3 COUNSEL'S CORNER**  
*By Chief (Ret.) Michael D. Ranalli, Esq.*
- 6 BUILDING A BODY CAMERA REVIEW POLICY**  
*By Professor Scott Phillips, Buffalo College*
- 8 FBI SCHOOL INITIATIVE "THE SRO LIAISON PLATFORM"**
- 9 THE PUZZLE PIECES OF CYBERSECURITY**  
*By Holly L. Hubert, FBI Ret., CISSP, CISM, CGEIT, CRISC*
- 11 NEW YORK VIOLENT DEATH REPORT SYSTEM (NYVDRS)....KEEPING DEATH RECORDS CONFIDENTIAL?**
- 12 BUILDING STRONG COMMUNITY RELATIONS THE BUFFALO POLICE DEPARTMENT NEIGHBORHOOD ENGAGEMENT TEAM**  
*By Lt. Craig Macy Buffalo Police Department*
- 15 IS RUNNING ALWAYS THE BEST OPTION?**  
*By Chief Stuart Cameron - Chief of Department Suffolk County Police Department*
- 18 WHY LEADERS LOSE GOOD PEOPLE**  
*Reprinted with the approval of the FBI Law Enforcement Bulletin*
- 19 CONFRONTING TERRORISM IN NEW YORK STATE**  
*By Robert Gardner, Senior Investigator of the New York State Police*
- 20 BULLETPROOF VEST PARTNERSHIP: WHAT YOU NEED TO KNOW TO RECEIVE FEDERAL FUNDS**  
*By Michael Schiller*
- 21 TECHNOLOGY UPDATE**
- 23 STRATEGIC PLANNING FOR SMALL LAW ENFORCEMENT AGENCIES**  
*By Chief Jonathan B. Flores, P1 Contractor*

## New York State Association of Chiefs of Police

### Staff

*Executive Director*  
ASST. CHIEF JEFFREY MORRIS  
PORT WASHINGTON POLICE DISTRICT (RET.)

*GTSC Liaison*  
DOMINICK G. MACHERONE  
DEP. CHIEF (RET.) GLENVILLE PD

*Director of Research, Development, and Training*  
CHIEF LARRY EGGERT  
LOCKPORT PD (RET.)

### Board and Officers

*President*  
CHIEF JOHN ARESTA  
MALVERNE POLICE DEPARTMENT

*First Vice President*  
CHIEF PATRICK PHELAN  
GREECE POLICE DEPARTMENT

*Second Vice President*  
CHIEF TIM PARISI  
ILION POLICE DEPARTMENT

*Third Vice President*  
CHIEF KEVIN SYLVESTER  
OSSINGEN POLICE DEPARTMENT

*Immediate Past President*  
CHIEF MICHAEL LEFANCHECK  
BALDWINVILLE POLICE DEPARTMENT

*Past President*  
CHIEF DAVID ZACK  
CHEEKTOWAGA POLICE DEPARTMENT

*Zone 1 Rep.*  
CHIEF MARTY FLATLEY  
SOUTHOLD POLICE DEPARTMENT

*Zone 2 Rep.*  
COMM. KENNETH O. JACKSON  
GARDEN CITY POLICE DEPARTMENT

*Zone 3 Rep.*  
ASST. CHIEF SEAN MONTGOMERY  
MTA POLICE DEPARTMENT

*Zone 4 Rep.*  
CHIEF GREGORY AUSTIN  
RYE BROOK POLICE DEPARTMENT

*Zone 5 Rep.*  
CHIEF JOSEPH SINAGRA  
SAUGERTIES POLICE DEPARTMENT

*Zone 6 Rep.*  
CHIEF PETE FRISONI  
SCOTIA POLICE DEPARTMENT

*Zone 7 Rep.*  
CHIEF THOMAS WINN  
CAMILLUS POLICE DEPARTMENT

*Zone 8 Rep.*  
CHIEF F. MICHAEL CATALANO  
CORTLAND POLICE DEPARTMENT

*Zone 9 Rep.*  
CHIEF SHAWN HEUBUSCH  
BATAVIA POLICE DEPARTMENT

*Zone 10 Rep.*  
CHIEF JAMES MICHEL  
LACKAWANNA POLICE DEPARTMENT

*Retired Member Rep.*  
CHIEF (RET.) JOSEPH DEL BIANCO  
MAMARONECK POLICE DEPARTMENT

*U.S. Attorney's Liaison*  
CHIEF (RET.) SAMUEL PALMIERE  
TONAWANDA POLICE DEPARTMENT

A publication of the  
New York State Association of Chiefs of Police, Inc.  
24 Century Hill Drive Latham, New York 12110  
Office: 518-355-3371

Do you have an interesting law enforcement story or an article you would like to submit, photographs of member activities or field scenes?  
Contact the editor: Larry Eggert at [leggett@nychiefs.org](mailto:leggett@nychiefs.org)

Copyright © 2019 • New York State Association of Chiefs of Police, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical or otherwise without prior written permission from the publisher.

The New York State Chief's Chronicle magazine is an official communication tool of the New York State Association of Chiefs of Police, Inc. The New York State Association of Chiefs of Police, Inc. does not assume responsibility for statements of fact or opinion made by any contributor. Comments made by individuals may not reflect the official position of the New York State Association of Chiefs of Police, Inc. Acceptance and publication of articles, advertisements, products and services does not indicate endorsement of same by the New York State Association of Chiefs of Police, Inc., and the New York State Association of Chiefs of Police, Inc. assumes no responsibility for their accuracy.

# On the Cover:

Buffalo Police Officer Jon Weber is seen playing kickball with neighborhood children in Buffalo, New York as part of the BPD Neighborhood Engagement Team. Sports related activities are only one method used by NET officers to build trust in parts of the city where families suffer chronic poverty and fear crime but whose trust in law enforcement is tenuous at best. According to Buffalo Police Commissioner Byron C. Lockwood, "I look at NET as being the model of the new Buffalo Police Department."

*Photo courtesy of the Buffalo News*

The New York State  
**Chief's Chronicle**



Serving New York's Police Executives Since 1901 March 2019



In This Edition:  
 Counsel's Corner  
 Feature Article - Building Strong Community Relations  
 FBI School Safety Initiative "The SRO Liaison Platform"  
 The Puzzle Pieces of Cybersecurity  
 Is Running Always the Best Option?  
 Confronting Terrorism in New York State  
 Technology Update



**INNOVATIVE THERAPEUTIC SOLUTIONS  
FOR LAW ENFORCEMENT**

**OFFICER BENEFITS**

- Decreased stress levels
- Pain relief
- Improved sleep
- Reduced muscle tension
- Enhanced relaxation

**DEPARTMENT BENEFITS**

- Decrease turnover rates
- Improve officer morale
- Small footprint
- Constructive way to cope with stress
- Decision making skills improve during highly stressful situations


**RESULTS**  
Symptom Decrease

Stress	Depression	Body Aches
57%	47%	54%
Muscle Tension	Headaches	
56%	44%	



**www.biosoundhealing.com | sales@biosoundhealing.com | 888-495-1946**

Phone (518) 370-5300 Fax (518) 370-5302



2 Freemans Bridge Road • Glenville, NY 12302  
www.TheWatersEdgeLighthouse.com

**M Matthews Auto**  
More. Every Day. Every Way.

**Kathy Breno**  
Marketing Director  
kbreno@matthewsauto.com

Matthews Auto Group  
PO Box 1130 • Vestal, NY 13851-1130  
t. 607.798.8000 • f. 607.584.0489 • c. 607.348.5503

**PROFESSIONAL FIRE RESTORATION**  
Specializing in Smoke, Soot and Water Removal



**Marc Giraudy** IICRC Cert.  
Supervisor

Albany (518) 452-1831 • Glens Falls (518) 792-4964  
Catskill (518) 943-0087 • Amsterdam (518) 842-5226  
(888) 358-9877 • www.pfrs.com

**When Only The Best Will Do**

**AARON LINDENBERG** SALES@ACCU-ROLL.COM  
GENERAL MANAGER



Suppliers of Precision Ground  
Rubber, Rubber Rolls and Metal Shafts

27 LOIS STREET ROCHESTER, NY 14606 PHONE# (585) 647-1997 FAX# (585) 254-4557

# Counsel's Corner



## Conclusive Evidence? Some thoughts on the Limitations and Influence of Video

Chief Mike Ranalli (Ret.) Glenville Police Dept.;  
Lexipol Program Manager



BY CHIEF (RET.) MICHAEL RANALLI, ESQ.

**A**n officer shoots an armed suspect, who later dies at the hospital. The officer is devastated but feels he did the right thing. The suspect's family mourns and protests that the shooting was unnecessary. The community demands answers. Then comes the Chief's press conference:

*"Our investigation has determined that the shooting by Officer Smith was justified. This finding is supported by Officer Smith's statement and the physical evidence. Ms. Suspect ignored the officer's commands to drop the knife and continued to move toward Ms. Victim in a threatening manner. Ms. Suspect then stopped and lowered the knife. Officer Smith then ordered Ms. Suspect to get on the ground, but she ignored his commands. Instead, she raised the knife and started to lunge toward Ms. Victim, causing Officer Smith to fear that Ms. Victim's life was in immediate danger. Officer Smith then fired his weapon three times to stop the threat. Ms. Suspect died from her injuries, but Officer Smith's actions were necessary and saved the life of Ms. Victim."*

And then the video is released, a video of poor quality taken from a neighbor's dated surveillance system. The police reviewed it as part of their investigation and did not see anything to contradict the statement of the officer and the physical evidence, including the relative locations of the knife and the victim. The public, and the attorney hired by the family to sue the department, see it as clear and compelling proof that Ms. Suspect was in fact moving away from Ms. Victim at the time of the shooting and did not lunge forward as stated by the officer. And, just to prove the point, the attorney releases "enhanced video" (zoomed in) which "clearly" shows the shooting is unjustified. Newspaper columnists watch the video and post their opinions that "it is clear from the video that the officer lied."

Now the tragedy expands. The department and the officer are vilified in the press: *The cops are trying to protect their own; they cannot be trusted to do their own investigations.* The officer is labeled a liar. Years of efforts of developing good community relations are destroyed in weeks.

### KISELA V. HUGHES

The initial facts regarding this scenario are very loosely based on a 2018 decision of the United States Supreme Court, *Kisela v. Hughes* (138 S.Ct. 1148 (2018)), with a few additional facts to make certain points clearer. The press conference and fallout from

the shooting are fiction but are also loosely based on several real incidents.

In *Kisela*, officers responded to a call of a woman, Amy Hughes, acting erratically and hacking at a tree with a knife. Upon arrival, officers saw Sharon Chadwick standing next to a car in a driveway. Hughes then came out of the house carrying a large kitchen knife and walked toward Chadwick. The officers had their guns out and were separated from the women by a chain-link fence. They commanded Hughes at least two times to drop the knife, but she kept it in her hand. Believing Hughes to be a threat to Chadwick, Officer Kisela fired at Hughes four times. The entire incident took about a minute.

Hughes survived her injuries and sued the department and the officers. The majority of the Supreme Court did not rule on whether *Kisela* violated Hughes' Fourth Amendment rights. Instead they ruled *Kisela* should have been granted qualified immunity since, under all these circumstances, *Kisela's* actions did not violate any clearly established law. Hughes was behaving erratically, possessed a large kitchen knife, moved within just a few feet of Chadwick, and refused commands to drop the knife. *Kisela* had to quickly make an assessment as to the potential threat to Chadwick based on the available information known to him at that time.

Two judges issued a strong dissent, ruling that a jury could find *Kisela* violated Hughes' Fourth Amendment rights. They relied heavily on the fact that only one of three officers fired, while the other two subsequently stated they felt they still had time to attempt verbal techniques. The dissenting judges also pointed out Hughes made no aggressive or threatening movements; she was just close to Chadwick, holding a knife she would not drop.

There was no video mentioned in the case, but since this decision was issued, I have wondered how video of the incident would have affected the outcome. Would it help or hurt the officer's case? What if the video showed Hughes was turning away from Chadwick at the moment she was shot? Would the ruling have been different? Would the video then be *conclusive* evidence the shooting was unjustified?

### THE PROCESS OF THINKING

A Google search of articles discussing the *Kisela* case revealed the following headline from the *New York Post*: "The Supreme Court just gave cops a license to shoot, then think."<sup>1</sup> While meant



to be sensational, this idea reflects the science behind System 1 and System 2 decision making.

The concept of two different and distinct methods of decision making has been around for some time, but it became more widely understood and labeled with the publication of a book entitled *Thinking, Fast and Slow* by Daniel Kahneman.<sup>2</sup> System 1 is fast, intuitive, emotional, automatic and heuristic-based. (Heuristics are mental shortcuts that we develop from previous experiences and problems.) System 2 is slower, deliberate and requires effort and attention.

Officers will be likely to rely on System 1 to respond to a rapidly unfolding, stressful situation. They will not always have all the information needed to make an educated and controlled decision. Instead they must rely on their experience, training and what they do know about the situation. Kahneman uses the phrase WYSIATI (What You See Is All There Is) to explain how we make decisions with System 1. We use the information available at the time. In potential life-or-death situations it may not be possible to engage System 2 by asking, “Hmmm, what do I not know?”

In our scenario, the suspect is moving toward the victim with a knife, refusing commands to drop it. She stops and lowers the knife but then lifts it up again and moves toward the victim. At that point, the intuitive System 1 response would be a predictable and automatic reaction to what is perceived as an imminent threat. But what about the video that shows the suspect was moving away from the victim at the time she was shot?

## UNDERSTANDING VIDEO ENOUGH TO KNOW YOU DO NOT UNDERSTAND VIDEO

Understanding digital video well enough to use it for more than general observations is difficult. It is an incredibly complex area. But the little bit I do know makes this clear: If the career or freedom of an officer—or freedom of a suspect for that matter—rests at least in part on the detailed interpretation of video, the agency should hire a forensic video expert. Period.

For purposes of this article I will attempt to explain just enough to understand the issue pertaining to our scenario. I have had the pleasure of attending several classes on video given by Grant Fredericks, the founder and owner of Forensic Video Solutions. One of the first points Fredericks makes is that the interpretation of video evidence is almost always based on bias. Proof of this can be found at any Super Bowl party where fans of both teams are watching. Just wait for the instant replay of a controversial call and see who lines up on either side of the debate.

Beyond bias, there are many other problems with relying on video as an accurate depiction of what the officer experienced. A video (even a body camera video) does not show you what the officer was seeing at the time. It provides a much broader picture beyond what the officer can focus their attention on. This is particularly true with third-party video off a house or building, such as in our scenario, or video taken by a bystander. The perspective can be completely different, creating the danger of assuming the officer saw something that may have not been visible or obvious from his or her perspective.

All video uses compression as part of the encoding process, creating another issue when video is used as evidence. This compression process uses prediction to reduce the amount of data, which results in the fabrication of data. Nearly all compression

algorithms are destructive, or “lossy,” meaning the lost data is generally unrecoverable. With DVRs, the compression rate may depend upon how long the data is to be stored. Also, file types such as AVI, MPEG, MP4 and WMV are all merely containers for digital data. The original proprietary file type unique to the source recorder is the best source of video. That is why video forensic experts say video that appears on YouTube is of no value forensically, because all metadata is gone.

Another issue arises with interlaced video, meaning two streams of captured video are encoded as one image. Again, this is a process that allows for smaller data transfers and storage, but when there is movement in the video, interlacing artifacts can be created. As a result, blurred and distorted images may be created that do not accurately depict the true motion. Certain nuanced movements by a person cannot be recorded by video. For example, in our scenario, if the suspect had visibly clenched the knife as she brought it up, gritted her teeth and quickly moved her body and the knife toward the victim before turning, the video would not necessarily reflect these movements. The source recorder may not have the resolution, or possibly the angle, to pick up on those details, and the faster the motion, the more likely it is the motion will not be captured.

Finally, zooming in on a poor-quality image in a video only makes the image bigger, not better. This does not “enhance” the video.

## THE IMPACT OF HINDSIGHT BIAS

I mentioned earlier that Fredericks underscores the effect of bias on video interpretation. Bias can be based on a person’s underlying beliefs and personal experiences. But there’s another bias that may be even more powerful, one the justices in *Graham v. Connor* tried to anticipate and prevent: hindsight bias. In our scenario, if Officer Smith had waited any longer, and the suspect was in fact intent on stabbing the victim, Officer Smith probably could not have stopped it. But in hindsight, that is not what happened and so there is a bias against the officer for not knowing at the time what the intent of the suspect was. What was learned after the shooting should be irrelevant to determining whether the officers’ actions were reasonable, but too often this knowledge becomes a factor.

While hindsight bias can be a factor in any use of force analysis, it becomes especially dangerous when video evidence is involved because we tend to assign video an unbiased perspective. The video has no reason to perceive things a certain way, after all. It’s not like an officer or a bystander or even an expert witness; it’s a machine. Fredericks and other forensic video experts can demonstrate that this is a flawed way to think about video, but the majority of the public continues to regard video as conclusive evidence.

The question that needs to be asked of the critics is, if the victim was stabbed while the officer did nothing, what would their attitude be then? If the victim was their sister, wife or daughter, what would they want the officer to do? The suspect was creating the situation, not the officer. Officers are thrust into such situations under high stress and must somehow correctly judge the intent of the person causing the risk. Officers must quickly judge what *could* happen, while the post-incident critics have the benefit of knowing what *did* happen.

In the *Kisela* case, the dissenting judges relied on the fact that

only one of the three officers shot as a reason to doubt the reasonableness of the force used. This is interesting because it begs the question, if all three officers had fired multiple rounds at Hughes and killed her, would the judges then have used that to find their actions excessive? If the officers had waited for indisputable proof that the suspect *was in fact* a threat, instead of just being reasonably perceived as a threat (which, by the way, is the law under the Fourth Amendment), and the victim was killed and then the suspect was shot, the tragedy would have been doubled. But hindsight bias can preclude that analysis.

## PUTTING IT ALL TOGETHER

When preparing press releases and briefings, police leaders need to be aware the issues involving video evidence. The language used in the press conference in our scenario is typical. While it is not wrong, it also may not tell the complete story. Using the standard Graham language—“at that point, the officer feared for his or her (or third party) life and the officer fired to end the threat” or some variation—can be misleading. It implies the officer had time to make a conscious decision and was in control of the situation. It also leads to the implication the officer should have known the suspect was no longer a threat.

This will not always be the case. Instead, the officer is relying on the subconscious and automatic process of System 1, which is reacting to all the information known to the officer at that time. The subtle and nuanced movements and facial expressions of the suspect, which may not be visible on a video, become subsumed within the rapid processing of System 1. Rapid and brief movements of the suspect may not be captured by video because of a different visual perspective or compression techniques that distort or blur images. As a result, video may not be conclusive evidence and instead could be misleading.

Police leaders also need to be aware of the concept of hindsight bias and understand that perception of video evidence can be affected by knowledge of the outcome of the incident. Many police executives and officers have learned to use *Graham* factors language when discussing use of force incidents. That’s good because it aligns what happened with established case law regarding use of force, but it may not be enough to explain apparent contradictions between video evidence and the officer’s account or the outcome of the investigation. It is impossible to suggest a one-size-fits-all approach, but some general considerations can assist police leaders when making a public statement following an officer-involved shooting. Some of these may or may not apply to your situation, but generally you should:

- Understand and accept that you cannot do this all yourself. Develop subject matter experts and trainers within your ranks and consult with them. Encourage debate and discussion about possible issues. If necessary, reach out to other agencies that have experts you may not. Thinking that you know everything you need to know can make things worse.
- Emphasize your explanation of the “high stress and rapidly unfolding” aspect of the situation. Many use-

of-force situations require officers to act automatically and responsively (System 1). Care must be taken to not create belief that the decision was conscious and deliberate if it was not.

- Address the dangers of hindsight bias head on. Keep the focus on the factors known by the officer(s) at the time of the shooting and remind the audience that anything learned afterward is irrelevant to the determination of whether the shooting was justified. If appropriate, discuss what could have happened but for the actions of the officer.
- Educate your audience about video’s limitations in perspective and image quality, but not just in general terms. If there are issues with the video from your incident, then both the technical aspects (e.g., method of compression) and the practical aspect (e.g., how that compression distorted an image) must be explained. If you use a forensic video expert during your investigation, ask them to help you develop these talking points.
- If applicable, emphasize that it is the suspect’s behavior and refusal to listen to commands that drove the incident.
- Do not make premature statements of fact before all the evidence has been reviewed.
- Do not wait for a tragedy to occur. Try to educate the public about these issues as much as possible before an incident occurs.

All the issues discussed in this article are assuming that the investigation finds the officer was justified in his or her response. If this is not the case, then police leaders face a much different conversation and of course, must take appropriate disciplinary action.

### (Endnotes)

<sup>1</sup> <https://nypost.com/2018/04/03/the-supreme-court-just-gave-cops-a-license-to-shoot-then-think/> last accessed January 23, 2019.

<sup>2</sup> Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY, US: Farrar, Straus and Giroux



# Building a Body Camera Review Policy

Photos Courtesy of Axon

BY PROFESSOR SCOTT PHILLIPS  
BUFFALO STATE COLLEGE

**D**uring the past few years there has been a growing call for “transparency” in policing. One of the primary reasons for openness in policing is because of their ability to use force, and the seemingly routine use of deadly force. There is, however, substantial research indicating that police officers use physical force infrequently, and the use of deadly force is incredibly rare. A prominent suggestion for improving transparency in policing is using body-worn cameras by street-level patrol officers and tactical officers. Body cameras are believed to be a tool for documenting the objective truth during an encounter between an officer and a citizen. Advances in technology, such as miniaturization of recording equipment and digital storage, make body-worn cameras a logical “next step” in police documentation equipment.

In addition to recording the objective truth of an officer – citizen encounter, police body cameras have several other goals. First, they are intended to improve the behavior of both officers and citizens during an interaction. Second, recordings can hasten the resolution of complaints against officers. Third, body camera recordings can be used as evidence in court. Finally, training can be modeled on behavior recorded by the cameras. Still, there are possible limitations in the utility of body-worn cameras. First, digital images can occupy a large amount of storage space on computer servers, which can increase the cost to police agencies. Second, there are privacy considerations on the part of the public. For example, bystanders, children, and emotionally or embarrassing events can be captured on cameras and become publicly available because digital images are the equivalent of public documents.

An unintended consequence of policy body cameras is their influence on the behavior of police officers. Research in Arizona found that police officers who were wearing body cameras were concerned that their supervisors would use the recordings to monitor officer’s activity, regardless of the agency’s policy against such inspections. The officers thinking resulted in behavior characterized as “risk aversion;” they wrote more traffic citations whenever they stopped a motorist to avoid supervisors questioning why they did not write a ticket.

The acceptance of body cameras in policing will be maximized if the officers interpret the technologies as being beneficial to their well-being. Police administrators will have to approach these tools in a manner that gains “buy in” from the patrol officers. Recent research in the Buffalo and Rochester Police Departments found that approximately 96 % of officers in both cities agree that when documenting a critical incident, they should be able to review body camera video. For example, if an officer is involved in a shooting, they feel they should have access to any video evidence while writing a report about the event. With that level of agreement police administrators could reasonably expect officers to accept body cameras if the agency’s policy allowed officers to review video evidence when writing a report.



Still, while the opportunity to review the digital images is strongly accepted by Buffalo and Rochester officers, research in other cities indicates disagreement among police administrators as to whether an agency’s policy should allow officers to review video evidence when writing a police report.

The fact that police officers wish to review video evidence when documenting an event is understandable; watching a video of what occurred can confirm incident details and insure an accurate report from the officer. Police administrators, however, must be aware of a few serious issues when developing a policy about allowing an officer the opportunity to review body camera images prior to

**There is a large body of research indicating that critical incidents or high-stress events can lead to perceptual distortions by those who experience the incident.**

writing a report. These considerations are particularly relevant when officers experience a critical or stressful incident.

First, it seems reasonable to believe that a policy preventing an officer from previewing video images when writing a report will result in documentation that includes variations from the objective reality of the event. That is, the officer’s report may not accurately reflect the reality of the incident. If this occurs, it is assumed that the officer is lying because their report does not match the video. This assumption is obviously false. There is a large body of research indicating that critical incidents or high-stress events can lead to perceptual distortions by those who experience the incident. For example, a person may experience events and not correctly interpret what they hear or see. In addition, people can develop false memories of what occurred; when a person experiences a critical incident, they may mis-interpret portions of the event, and the memory fills in the missing pieces with logical conclusions. Simply stated, perceptual distortions and false memories can cause people to believe they see or hear something that did not, in fact, occur. For example, one of the New York City police officers

—*BUILDING A BODY CAMERA, continued on page 7*



involved in the 1999 shooting of Amadu Diallo believed he saw a gun that was actually a wallet.

Regardless of the perceptual distortions and false memories, an officer's interpretations are genuine, and can be a justification for their use of force, even deadly force. Therefore, if a police officer is required to write a report prior to reviewing body-worn camera images and explains the rationale for their decision or action

**The problem is that an officer may focus solely on what is recorded by the camera and accidentally forget what they saw but what was not recorded.**

based on their perceptions and beliefs, this would be a good-faith explanation. That is, the officer is telling the truth based on their perception of the event even if their narrative does not match the video evidence.

On the other hand, if the officer is allowed to make a statement or write their report commensurate with viewing the camera images, it is possible that the digital video will not comport with the officer's original perceptions and memory of the event. For example, the officer may have believed they saw a weapon, and used force as part of a good faith decision based on that perception. The video, however, may clearly show a cell phone. In this case the police officer's use of physical force cannot be justified because a cell phone is not a weapon. The officer's original justification for the use of force is now lost. In that case the officer may adjust their report narrative to fit the video, or the

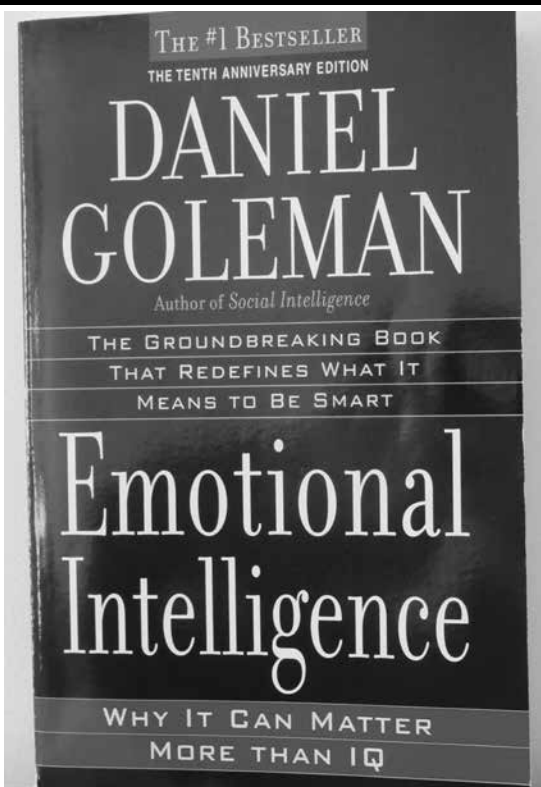
officer may alter their explanation for justifying their behavior. In either case the officer is now lying on their report because they are not telling the truth as they first understood it. Essentially, if a police agency has a policy allowing officers to review video images prior to writing a report, the policy may result in an officer committing perjury because their written statement is different from what actually occurred.

A second important consideration when developing a body-camera review policy deals with "retrieval-induced forgetfulness." It is argued that when a police officer reviews the images from a body camera, they will construct a narrative based on the information available on the video. This is not necessarily a problem, as the video images likely contain information that the officer may not remember. The problem is that an officer may focus solely on what is recorded by the camera and accidentally forget what they saw but what was not recorded. Basically, a true memory of events vanishes when not confirmed by the video.

Overall, police administrators who have developed a body-camera policy, or are considering such a policy in the future, must deliberate on these issues. The problems discussed here must be explained directly to the officers impacted by the policy, as well as local politicians and the public. The research on perceptual distortions, false memories, and accurate recall, must be included in the policy debate.

*Scott W. Phillips is a Professor in the Criminal Justice Department at Buffalo State College. He worked as a police officer in Houston, Texas and for the COPS Office in the Department of Justice. His research interests include police officer decision making and organizational influences on officer's behavior.*

## BOOK REVIEW



Everyone knows that high IQ is no guarantee of success, happiness, or virtue, but until *Emotional Intelligence*, we could only guess why. Daniel Goleman's brilliant report from the frontiers of psychology and neuroscience offers startling new insight into our "two minds"—the rational and the emotional—and how they together shape our destiny.

This book illustrates that the single most important factor in any human venture, especially leadership, is not the level of intelligence of a person, college degrees or technical knowledge. Rather it is the quality and level of a person's "Emotional Intelligence". Through vivid examples, Goleman delineates the five crucial skills of emotional intelligence, and shows how they determine our success in relationships, work, and even our physical well-being. What emerges is an entirely new way to talk about being smart. The new "smart" is how we handle ourselves and each other.

The good news is that we are not born with a fixed level of "Emotional Intelligence". Instead, Goleman identifies that we all possess the potential to improve our Emotional Intelligence at any time in our career or level of leadership. Each of us as parents, teachers, and leaders have a stake in this compelling vision of human possibility.

As you will discover in your reading, emotional intelligence does not mean merely "being nice," but rather, for example, bluntly confronting someone with an uncomfortable but consequential truth they have been avoiding. Emotional Intelligence also does not mean free expression of emotions. Rather, it means managing and expressing feelings appropriately and effectively to build relationships to get the job done.

# FBI School Safety Initiative “The SRO Liaison Platform”

BY FBI SPECIAL AGENT DAVID BUDZ

Impacted by the dramatic increase in school shootings, law enforcement agencies and school administrators have realized a common goal: protect students and employees during potential mass casualty events. Working as a team with a clear-cut vision, the two groups have developed multiple paths towards safety successes in area school districts. Staffing additional school resource officers (SROs), securing every building, preparing coordinated training, addressing gun ownership, and controlling access to campuses are just some of the issues at the forefront of efforts to protect school campuses that were once singularly designed for learning.

## SRO LIAISON PLATFORM

While law enforcement and private sector groups have been proactive in preparing threat assessments and providing active shooter training to best-ready school staff, the lingering question remained: how do we adequately equip and aid SROs who are alone on the front line of defense? The FBI in Buffalo sought to answer that question when it developed a multi-level liaison platform with a unique focus to specifically support SROs. Through the platform, officers in the 17 counties of Western New York (WNY) address issues surrounding school violence. This liaison concept has not only proven successful, but it has allowed for the development of mutual trust among primary stakeholders, including officers, chiefs, sheriffs, agents, investigators, and community partners.

The SRO liaison platform, which has two levels, has provided a venue to raise concerns and share best practices. The base level of the platform is an email group linking dozens of regional SROs who use the network opportunity to share information, pose questions, push out intelligence, and organize briefings to study past and current threats.

## SRO BRIEFINGS

The upper level of the liaison platform provides for face-to-face communication at SRO briefings. It can also serve as a forum for school administrators and community partners. As a lead intelligence agency, FBI Buffalo provides opportunities for law enforcement in its region to engage at productive briefings and achieve the unified goal of all partners in attendance. Having the unique ability to organize gatherings spanning multiple jurisdictions, FBI Buffalo has begun facilitating two to three SRO briefings annually, starting in 2017. Keeping with the overall mission of protecting our schools, these briefings provide an after-action forum to discuss the difficult, yet valuable lessons learned from previous school attacks or threats. SRO briefings mirror the format of a traditional law enforcement tabletop exercise (TTX) and include reviews of real-life situations. Face-to-face SRO briefings produce healthy discussion and participants gain critical knowledge regarding best practices, collect informative materials, and receive insightful answers to address concerns in their respective school district. This connecting of law enforcement with community partners allows the proper personnel to examine various issues, vulnerabilities, and gaps. There is no substitute for the open dialogue and discussion. The benefits are immense and the connections could result in many lives saved in WNY.

The number of participants in the liaison platform has increased over time, and as a consequence, the intelligence value of the SRO briefings has grown. For example, at an SRO Briefing in December 2018, presenters shared the specifics of recent threat resolutions involving three local school districts. The lead investigators and administrators from each of the three districts provided detailed overviews of each incident. The first two incidents involved bomb



*FBI Buffalo Special Agent David Budz runs an after-action briefing in January of 2019 for the Letchworth Central School District SRO, school administrators, and law enforcement first responders in Wyoming County.*

threats at two school districts and the third incident involved a student at a WNY school who is alleged to have developed an elaborate plan to murder his parents, the SRO, first responders, and as many people in the school as possible. Law enforcement made arrests in each district before an attack occurred and all three threats were eliminated.

As the liaison platform initiative has advanced in WNY, FBI Buffalo has expanded the SRO briefing format to smaller venues to include individual school districts, administrators, staff, board members, local first responders, and related community partners. Discussion during these briefings has centered on two critical areas:

1. How are the district and law enforcement identifying and processing internal threats among the student population?
2. How is the district hardening its physical layout against outside threats attempting to gain entry into the school?

Law enforcement in WNY would like to see the liaison platform initiative become a model adopted throughout the nation to address an immediate need to equip and support SROs.

*About the author: Special Agent David Budz is a 17 year veteran of the FBI assigned to the Buffalo office. His current assignment is the Special Events/Mass Gatherings Coordinator and Tactical Operations Center Senior Team Leader. Prior to the FBI, Special Agent Budz worked for 7 years as an elementary school teacher.*



*Starpoint Central School District Superintendent of Schools Dr. Sean M. Croft (pictured left) and Niagara County Sheriff's Office Deputy and Starpoint SRO Craig Beiter highlight safety features of the district's video security system for FBI Buffalo Special Agent David Budz.*

# The Puzzle Pieces of Cybersecurity

BY HOLLY L. HUBERT, FBI RET., CISSP, CISM, CGEIT, CRISC

If you asked a group of American business owners and academicians at a dinner party who are the biggest cyber threat actors against organizations in the United States, I bet they would only mention Russia. They would not be wrong, yet that is only a fraction of the picture. We know about what we see and hear every day via news and social media. We receive daily doses about the Russian cyber threat and much less about other threat actors. Every minute of every day, businesses and organizations in the United States face threats from China, North Korea, Iran, and other foreign governments that have highly sophisticated nation state-sponsored hacking corps as well as other criminal organizations and individual threat actors. Why? Because sophisticated hackers can raise incredible amounts of money, acquire private financial data, and steal intellectual property, threatening our very American way of life. In a country built on ingenuity, capitalism, and work ethic, our very livelihoods are at stake. Every day we read or hear about a major company experiencing a data breach in which our private financial or health care data is spilled. The collective economic loss every year is staggering, reaching into billions of dollars. We are all very aware of attacks on small/medium/large organizations, hospitals, school districts, and even police departments.

To complicate further, the myth that hackers are only looking for billion-dollar high-profile targets permeates small and medium-size business culture. According to 2018 Small Business Administration data, 99.9% of businesses in America are considered “small.” Hundreds of the 30.2 million businesses may be located in your villages, towns, cities, and municipalities. The organized cyber-criminal or state-sponsored foreign threat actor uses automated tools to scan the Internet for any vulnerabilities making their targets simply “opportunistic.” They are not aware of corporate gross sales, bottom line, or number of employees. They are looking for one thing: openings! Can they get in?

According to Verizon’s 2018 Data Breach Report which includes the analysis of over 2,200 data breaches that occurred throughout 2017:

- 76% of breaches were financially motivated
- 12% were perpetrated by state-sponsored actors
- 28% involved insiders
- Ransomware is the top variety of malicious software (malware)
- 68% of breaches took months or longer to discover

## FROM A LAW ENFORCEMENT PERSPECTIVE, WHAT CAN WE DO ABOUT THESE THREATS?

How can law enforcement mitigate this problem? First, as a local, state or even federal law-enforcement officer, it is nearly impossible to arrest a target that is in Russia, China, North Korea, etc. What law-enforcement can and should do is join their local FBI Cyber Task Forces. The FBI is the lead federal agency for investigating cyber-attacks. These task forces are nationally coordinated and give local law enforcement agencies a seat at the table on a national level. Even though the perpetrators of cyber-crime usually reside outside of the United States, the victims are in our towns and municipalities.

The second way state and local law enforcement can address cyber-attacks is by proactively educating local businesses on prevention. Take an approach similar to community policing. Be active in the business community in providing cybersecurity tips and best practices. Engage subject matter expert speakers in local forums to educate businesses on cyber threats and mitigation strategies in three broad areas:

1. Hardening their Information Technology (IT) posture
2. Train employees to recognize nefarious emails and other cyber threats
3. Having a practiced incident response plan that includes recovering from back-ups to minimize the attack and recover as quickly as possible.

It may seem cliché, but organizations should strive for as “hard” of an IT posture as possible. Threat prevention can be a daunting task, particularly for a small and medium business, often with no onboard IT employees. The language of cybersecurity is complex and there is a tremendous skill-shortage. Individuals within the IT industry get paid to make sure that corporate IT assets run the business. There are so many individual areas of expertise within “business IT,” that cybersecurity concerns are left usually under-



addressed or not at all. Within each business IT realm, there is individual cyber security expertise that is absolutely essential. It is normal for small and medium businesses to outsource their business IT needs to local providers which presents a laundry-list of additional concerns such as the competence, training, and experience of their employees on complex cybersecurity concerns; their access to customer critical/protected data; where they store customer passwords; the security of their remote access into customer environments; their competence and experience in restoring from customer backups; their employee vetting process; overreliance on one or two employees, etc. Even larger organizations with onboard cybersecurity personnel face the



GlobalSecurityIQ™



constant daily challenge of these dynamic ever-changing threats in a complex space with many commercial solutions.

A solid Cybersecurity Program is every bit like a puzzle with many pieces. Companies should identify their pieces utilizing the industry-preferred NIST-based Risk Assessment methodology. A comprehensive Risk Assessment will identify what elements are already in place and provide the organization with a list of missing pieces which are identified as risk areas prioritized by criticality. A comprehensive Cybersecurity Risk Assessment, conducted by an experienced and credentialed outsider for objectivity, is crucial and should be repeated at least annually.

A vulnerability scan of an organization's internal network, external network, and web-applications will identify misconfigurations, open ports, missing patches, and other critical vulnerabilities depending on the depth of the scans and the experience of the practitioner. 85% of data breaches can be prevented if companies mitigate identified risks and vulnerabilities. If law enforcement can nudge organizations into conducting comprehensive Risk and Vulnerability Assessments, they will do wonders in serving and protecting those enterprises in their respective communities.

Unfortunately, all breaches cannot be prevented. Companies should educate all employees on the recognition of nefarious emails and other cybersecurity risks. This education should include formal training as well as employee testing to anchor the learning. Cybersecurity should be the concern of all employees and weaved throughout the culture of the enterprise from the board-level down to line-employees.

Many companies believe that cyber insurance policies are the answer and they believe they are "covered." Insurance is a mere piece of the cybersecurity jigsaw puzzle to be considered in an overall security posture. Cyber liability insurance is very tricky. If the organization does not have a qualified person review the policy, they may not be covered for certain breach incidents. For example, a breach that originates from a social engineering attack is often

not covered unless it is specified in the policy. Many data breaches originate from employees clicking on a link or attachment in phishing emails. These breaches are considered social engineering attacks thus leaving an organization vulnerable when they believe they are "covered."

Finally, to address, the "not if, but when" data breach concern, all organizations should have an incident response plan. This plan should address the response by role to minimize the effects of a breach, effective recovery from backups, compliance reporting, a communication plan, and overall crisis management. An outside organization can help in crafting such a plan to ensure that it is thorough and leverages crisis management experience. This plan should be tested on a minimum-annual basis to ensure that all key individuals understand their respective roles and can confidently execute them in a pressurized situation.

Cybersecurity is indeed a jigsaw puzzle. Law enforcement agencies can be key partners to local businesses by facilitating educational offerings. Organizations should always start with an outside Risk Assessment and Vulnerability Scan. The identified risks will guide the other pieces to help craft a meaningful and measured Cybersecurity Strategy.



*About the author: Holly L. Hubert is a 25-year FBI veteran. As an FBI Supervisory Special Agent, Hubert founded the FBI Buffalo Division Cyber Task Force and directed the establishment of the Western New York Regional Computer Forensic Laboratory. Retiring in 2017, Hubert founded GlobalSecurityIQ, a Cybersecurity and Risk Mitigation firm. GlobalSecurityIQ specializes in Cyber Risk Assessments, Vulnerability Scanning/Penetration Testing, Incident Response, Digital Forensics, Education, and Leadership Consulting. [www.GlobalSecurityIQ.com](http://www.GlobalSecurityIQ.com)*



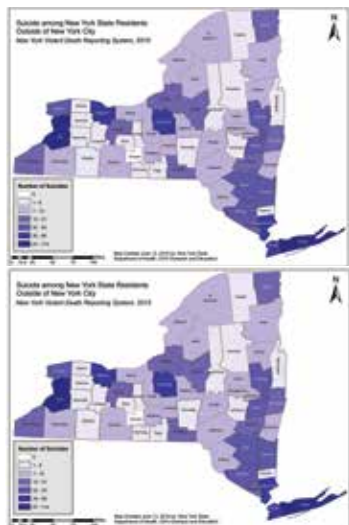
**FOLLOW US ON TWITTER:**

**@nysacop**

# New York Violent Death Report System (NYVDRS).... keeping death records confidential?



BY KIMBERLY FRIELLO  
PROJECT MANAGER, NYVDRS



Violence remains a major public health problem. The economic impact is staggering, with suicides costing the U.S. economy \$50.8 billion and homicides \$26.4 billion. In 2016, 2,389 people died violently in New York State; that's an average of seven people each day. Of these violent deaths, 1,679 were suicide and 696 were homicide deaths. Suicide was the 12th leading cause of death among all ages, and the 2nd leading cause of death among persons

aged 10-34. Homicide was the 17th leading cause of death among persons of all ages in NY, and the 3rd leading cause of death among persons aged 15-24.

## NATIONAL SUPPORT OF THE NEW YORK VIOLENT DEATH REPORTING SYSTEM

To help find answers to preventing violent deaths, organizations and partners such as the American Public Health Association (APHA), National Association for Public Health Statistics and Information Systems (NAPHSIS) and the National Association of Medical Examiners support the Centers for Disease Control and Prevention's (CDC) and work in cooperation with the National Violent Death Reporting System (NVDRS). The International Association of Chiefs of Police (IACP) also supports and promotes increased awareness of, and agency participation in NVDRS by law enforcement.

We invite you to visit CDC's website at: <https://www.cdc.gov/violenceprevention/nvdrs/index.html>, for additional details.

## HOW DOES NYVDRS KEEP DEATH RECORDS CONFIDENTIAL?

NYVDRS data are collected under the same federal security and confidentiality guidelines that govern surveillance activities and no personally identifiable information is collected in the NYVDRS.

The NVDRS software and databases are maintained directly by CDC in federal facilities. NVDRS is operated in compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." The NVDRS System Security Plan is reviewed annually by CDC's Office of the Chief Information Security Officer, which also conducts continuous monitoring of the NVDRS servers and databases.

State health departments submit information to CDC only

after removing all potentially personally identifiable information including; names, addresses, and dates of birth. Participating

**It is important to receive accurate data as state and local violence prevention practitioners use the data to guide prevention program, policies, and practices.**

NVDRS states and territories enter data into an encrypted web-based system. The names of individual victims and suspects are not released at the state level. Local laws that protect other types of health department records, such as communicable disease records, also apply to NVDRS files.

NYVDRS receives information from county Coroners as they are mandated reporters. However, our organization also must manually request death information from individual police departments for any violent deaths. This manual requesting is sometimes not fulfilled, which precludes our organization from accurately collating data for dissemination. It is important to receive accurate data as state and local violence prevention practitioners use the data to guide prevention program, policies, and practices.

Please note that acquisition of patient information and compliance with HIPAA follows the federal regulation, 45 C.F.R. Part 164.512 which authorizes disclosure in many circumstances, including the following:

Disclosure is permitted to a public health authority authorized by law to access information to prevent/control disease, injury, and disability, e.g., disease reporting, vital statistics reporting, public health surveillance, public health investigations, public health interventions and partner notification.

All staff involved with the project understand the sensitivity of these documents and no personal information is released into the realm of public knowledge. As employees of the New York State Department of Health, we are required to take confidentiality training, and appropriate procedures are followed to ensure only those involved in the project have access to the personal identifying information, and that all information is maintained in a secure environment. No personal identifiers are entered into the CDC data collection system, nor are personal identifiers ever released to an outside party.

During the 15 years of NVDRS data collection nationwide, there has never been a data breach or compromise of the confidentiality or security of the system. NVDRS has been in existence since 2002 with six states initially participating. As of 2018, NVDRS data collection expands to all 50 states, Washington D.C., and Puerto Rico. This is a true testament to all the hard work, dedication, and continued support of our Data Partners.

# Building Strong Community Relations

## The Buffalo Police Department Neighborhood Engagement Team

BY LT. CRAIG MACY BUFFALO POLICE DEPARTMENT

In June 2018 Buffalo Police unveiled a 100 day detail with a focus on building stronger community relations, which in turn would improve the attitude towards police in the communities we serve. This idea, which was conceptualized by Buffalo Police Commissioner Byron Lockwood and Buffalo Mayor Byron Brown, called for our Officers to meet regularly with citizens on a personal level. All too often police only deal with the citizens during a time of crisis; in an emergency; or when they are involved in-or are the victim of a crime. How do we positively engage the large part of the population that has little or no regular and positive interaction with the police? How do we build strong relations with the people that have so much information on the daily events that occur in

**Flexibility is one of the keys to success when looking at how to better improve relationships with each unique community.**

their neighborhoods? We do this through positive interaction, achieving results, professionalism and community policing. The Neighborhood Engagement Team (NET) was created by the Buffalo PD to bolster our existing Community Policing Program. The Community Policing Program had existed in each of our 5 Patrol districts for the past several years. Unlike the district Community Police Officers (CPOs), NET Officers have two specific tasks: Build positive, strong police/community relations; and practice Problem Oriented Policing. NET officers operate with very few restrictions on how to accomplish their mission.

Due to the initial success of the program, the Neighborhood Engagement Team became permanent in October 2018. The current makeup of the NET consists of two platoons, each with one Lieutenant and five officers working the afternoon shift to continue to build on the program's initial success. NET focuses on a specific neighborhood(s) for approximately two months at a time. During the process to select a neighborhood, officers look at quality-of-life complaints, crime trends and other relevant data. By summer of 2019 NET will have been in every district in the City. Once a neighborhood has been selected, team members work with community members to achieve the objectives of the program. Buffalo is a very diverse city, with many cultures, languages and customs. With that diversity comes many different concerns regarding what constitutes quality of life and crime problems. These problems can vary significantly for each neighborhood.

Flexibility is one of the keys to success when looking at how to better improve relationships with each unique community. Another key to success is being able to use that flexibility to successfully address crime, quality-of-life concerns and other problems specific to the individual area.

One of the key facets to success of the NET is the partnerships that have been built with community groups, government sector agencies, and our partner law enforcement agencies. It is these partnerships that allow our officers to more effectively enforce the

law while using those enforcement efforts to improve the quality of life for each neighborhood that we visit. Allowing our officer's time to walk in each detail area with no other objective or obligation

**Youth events have been a cornerstone for the NET program.**



**Buffalo Police Officer Jon Weber is pictured playing kickball with neighborhood children as part of the NET program.**

*Photo courtesy of the Buffalo News*

besides talking to residents and being available has been greeted in a very positive manner by the residents of the neighborhoods. This personal interaction generates all manner of information regarding the different concerns and problems of that area. Many of these concerns are new to the officers and probably would not have come to light without this personal touch. This type of interaction has been good for both the police and the residents. The police can do the police work that the residents desire. In turn, the residents feel safe, realize the police care about their problems, and are empowered by their input with the police.

Youth events have been a cornerstone for the NET program. During the warmer months, Officers regularly hold and organize pick-up football, soccer and kickball games in vacant neighborhood lots. These nightly events had the support in both attendance and participation by both Mayor Brown and Police Commissioner Lockwood. In the colder months, for which Buffalo is famous, our outreach moves into local community centers where we host various sports programs with the goal of maintaining our presence in the community and continue to build positive relationships. Our program also arranges for attendance at local professional sports games throughout the year. We are lucky in Buffalo to have professional football (the Bills), hockey (the Sabres), lacrosse (the bandits) and baseball (the Bisons) teams for year-round opportunities



for our kids. Attending these professional sporting events with our Officers have provided a long lasting positive outlook on the Buffalo Police Department for the many children and young adults in our program. Most may have never left their own neighborhoods or the City limits during their lifetime. Attending sporting events presents a world view they otherwise may never experience. Also, providing rides in a marked police car and sitting with some cops at a Bills game can help change their perspective on the world as well. As part of our continuing interaction, officers stress the importance of school and education at weekly after-school mentor and homework sessions. Events like these are invaluable when it comes to the quality time spent with our Officers.

One of our community partners is the Erie County District Attorney's office. During our regular evaluation of NET program, we discovered less than desired results associated with our effect on quality-of-life crimes. We approached our county District Attorney, John Flynn, and informed him about the mission and objectives of the Neighborhood Engagement Team. He quickly put both his support and the support of his office behind the NET unit, assigning a full time Assistant District Attorney to our staff. These ADA's have provided training to officers and regularly attend NET community meetings, which has been very helpful in explaining the legal process to residents. Through this initiative our community relationships and overall program results have strengthened and improved.

Another of our program partners is the New York State Police Community Narcotics Enforcement Team (CNET). CNET has been valuable in addressing the street level drug sales that have plagued some of our neighborhoods. NET officers hold regular meetings with CNET, the BPD Intelligence Unit and the assigned Erie County ADA to address resident concerns, build strategies to address identified concerns, and follow up on existing open cases. As an example of the effectiveness of this partnership, in a one-month period, our uniformed NET officers: Obtained and executed two vehicle search warrants; recovered well over 1 pound of marijuana packaged for sale; made several arrests involving the possession of felony level crack cocaine and the sale of marijuana; and seized over \$17,000 in currency. While this is not our normal arrest output on a monthly basis, it is a good indicator that our partnership and resulting investigative methods are working very well. These results are in addition to on-going long-term investigations with our Federal partners that once completed will dismantle a network of street dealers that have devastated specific areas of our city.

One of the biggest achievements for a community policing unit is when law abiding citizens come forward with information. A major hurdle police face daily when investigating crime is the "code of the street" or "snitches get stitches". This creates fear in ordinary citizens and gives them an understandable reason not to talk to the police. Casually talking to citizens at different times has led to NET Officers recently obtaining very specific information on two open homicide cases. Suspects were named, and social media account information was provided. The sharing of this information was a direct result of spending several days simply walking around an assigned area talking to as many people as possible, building a good rapport with the community, and thereby building a network of people willing to assist our law enforcement efforts.

The opportunities for NET to build on our early successes continue to expand with the increasing levels of community acceptance and support. This summer (2019) we plan to use existing community partners "Victory Sports" and the Buffalo Police Athletic League to



**BPD Officers playing with neighborhood children as part of the NET program.** Photo courtesy of the Buffalo News

build new partnerships with groups like Go-Bike Buffalo and Slow Roll to expand our reach into the community and reach a larger percentage of City residents. We anticipate weekly attendance at Slow Roll and to expand nightly sporting activities and games with community youth. In conclusion, our Neighborhood Engagement Teams will continue to expand our reach into the community, explore new methods, and generate new opportunities with the goal of making the City of Buffalo a safe place to live, work and raise our families.



**NET Officers listening to residents concerns as they walk through a neighborhood.** Photo courtesy of the Buffalo News

## NET Neighborhood Engagement Team



**WE OFFER FHA LOANS**  
with as little as **3.5% down**  
and **VA loans** with **NO DOWN**  
**PAYMENT REQUIRED.**



**Nationwide**  
Mortgage Bankers Inc.

Your job is stressful, financing your home shouldn't be. We are committed to making the process easy so you can use your time to worry about more important things.

- No processing fee.
- No application fee.
- No commitment fee.
- No document prep fee.
- No junk fee.
- No underwriting fee.
- Reduced attorney fees.
- We do out-of-state loans.
- Competitive rates.
- Direct lender.

MORE INFO

**800-370-POLICE (7654)**

EMAIL

[nyschiefs@nmbmortgage.com](mailto:nyschiefs@nmbmortgage.com)



*Registered with the Nationwide Mortgage  
Licensing System NMLS # 819382*



# Is Running Always the Best Option?

*Pictures Courtesy of Chief Stuart Cameron*

BY: CHIEF STUART CAMERON – CHIEF OF DEPARTMENT SUFFOLK COUNTY POLICE DEPARTMENT

Concerns over school safety have changed drastically in recent years as the prospect of a mass shooting occurring within any given school facility have increasingly garnered attention. School administrators who were trained primarily to educate students are now faced with implementing effective security plans to protect students and staff. Many of these administrators will seek guidance from their local law enforcement agency as they pursue enhanced security within their buildings. Law enforcement agencies must be prepared to assist in this endeavor by providing valid and effective guidance in an attempt to harden these potential targets and reduce these risks.

In 2012 a team of individuals in the City of Houston who were working on a Department of Homeland Security funded initiative to foster regional disaster planning created the now widely recognized Run, Hide, Fight mantra. This phrase and the professional quality video that was made as part of this same effort were a huge step forward for the general public with respect to active shooter preparedness. The simple, easy to follow guidelines provided a sound strategy for the average citizen in the unlikely event that they became involved in an active shooter event. The setting for the Run, Hide, Fight video appeared to be a corporate

**Panic, inaction or indecision by a single member of the group at any point along the way could jeopardize everyone's life,**

environment populated with adults who could individually heed the advice contained in the video. Rather than react as a deer caught in the headlights, those who adopted the Run, Hide, Fight mindset could immediately act to save themselves and those around them, provided their co-workers were willing to obey the guidance as well. The video made it clear to encourage those around you to run with you, but not to be slowed down by those who refused to come along. As stated clearly in the video, "encourage others to leave with you, but don't let them slow you down with indecision."

Some schools have now begun adopting the Run, Hide, Fight strategy as well. How will this approach transition from the original corporate setting into our schools? Clearly there are some significant differences between these two environments including the age of those occupying each space and the fact that teachers are responsible for the safety of the children in their care and simply do not have the option to leave indecisive or hesitant students behind. Moving as a cohesive group out of a threat environment would also be significantly more challenging than attempting to exit the situation alone or in small groups. Panic, inaction or indecision by a single member of the group at any point along the way could jeopardize everyone's life, especially given the fact that no student can be separated from the group or left behind. There is also little doubt that a teacher with a group of school children could never be as quiet, agile and quick to respond as an adult could while moving solo.

Mass shooting attacks at school facilities have occurred at varied times in the school day and at a variety of locations throughout school buildings. For example, attacks have occurred at the start and end of the school day when students are not generally within their classrooms, but rather clustered together in groups in hallways and other open areas. Additionally large gathering areas, such as cafeterias, gymnasiums and libraries have, often by design, been the site of carnage in the past. It has been reported that Eric Harris and Dylan Klebold spent time prior to the Columbine attack in an effort to determine the time during each day when the most students would be present in the cafeteria, so they could maximize the impact of their initial attack. Ultimately Klebold and Harris would go on to injure numerous students in the school's library, another large gathering area. Kip Kinkel, a school shooter, who acted prior to the Columbine event in Oregon State, also targeted students in the school's cafeteria. These types of open mass gathering areas possess numerous entrances and are far more challenging to protect when compared to a conventional classroom. Attacks have also been launched when students were within their classrooms. How would the Run, Hide, Fight strategy apply in these varied settings and would it be a successful model to follow regardless of the age and grade level of the students involved?

Most school facilities have been implementing lockout and lockdown procedures for many years. A lockout involves securing all exterior entrances to prevent a threat that is outside the building from entering. Many schools restrict access during the school day to a







## —IS RUNNING ALWAYS THE BEST OPTION? from page 15

single visitor entrance which allows a lockdown to be established in a very rapid manner by simply locking the visitor entrance or by restricting access to a door that is already kept locked until the event is concluded. A lockdown is much more restrictive and is designed to protect or shelter students and staff members from a threat that may already be within the building. A lockdown configuration would involve classroom doors being closed and locked with students moved to be out of sight from the hallway. Some schools advocate that lights be turned off and blinds be closed, while others do the contrary, leaving lights on and blinds open.

The decision to adopt a run, hide, fight strategy as initially developed by the City of Houston should not be taken lightly for schools. Once an event of this nature begins preplanning and preparation could very likely mean the difference between life and death for the children or young adults in the involved facility. The video produced by the City of Houston portrays the run, hide, fight model as linear in nature, wherein leaving the facility should always be the first option considered. As the video clearly states “first and foremost, if you can get out do, always try to escape or evacuate, even if others insist on staying”. This guidance may be appropriate for students and staff directly exposed to an active shooter in the facility, whether the attack occurs during change of classes or in an open mass gathering area, such as a cafeteria, gymnasium or library where rapidly moving away from the threat would be a basic act of self-preservation. However, in instances where students are within classrooms that have been or could be rapidly configured into a lockdown mode should running always be the initial option to consider?

When lives are on the line, especially the lives of school children, it is best to make evidence based decisions and to extensively study how previous attacks have unfolded to determine which strategy has provided the best overall protection. A report produced by the Sandy Hook Advisory Committee, a sixteen member committee empanelled by the governor of Connecticut to examine the Sandy Hook School shooting, clearly stated that no active shooter in a school facility has ever breached a locked classroom door. This fact clearly bolsters the conclusion that the lockdown model, when rapidly and properly implemented, may be the safest option for students who are already within classrooms when an active shooter attack begins.

Since active shooter attacks generally occur without warning and evolve quickly, prompt notification to initiate a lockdown is essential for this strategy to be effective. When Adam Lanza attacked the Sandy Hook elementary school in December of 2012 his immediate focus on the administrative staff and the school’s main office may have prevented a school-wide lockdown notification from being made. After the event had concluded some staff members reported hearing noises when the attack began, but many did not recognize them as gunshots. The classroom in the school where the greatest carnage occurred that day was staffed by a substitute teacher who may have been less familiar with school security protocols as compared to permanent teachers and may not have had a room key as readily available. Additionally doors locks at the school required that the key be inserted on the hallway side of the door. There was no means to lock the door from the inside complicating rapid action under threat.

Best practice recommendations for classroom door locks include the ability to lock the door from the inside without having to open it. Requiring a key to lock the door from the inside would prevent unauthorized people from locking the door and potentially locking staff members outside of the room, but it could also slow the pace of this process during an attack and require fine motor skills under incredible stress. Generally all staff members should be issued keys for the rooms that they work within and the keys should be carried at all times to facilitate rapid action when required. Additionally the glazing within classroom doors could potentially be a weak link. Efforts should be made to prevent the breaching of the door glazing from allowing the door lock to be compromised.

Much like the Sandy Hook Elementary School, students and staff members in Virginia Tech’s Norris Hall reported hearing strange noises when Seung-Hui Cho began his attack there in April of 2007. An ongoing nearby construction project had been generating loud noises for an extended period prior to that fateful day, so many assumed the noise was coming from that source. Cho’s attack focused on five classrooms on the second floor of Norris Hall. He entered some of the rooms multiple times; however efforts were made to deter his entry in two rooms. The door to one room was effectively barricaded with furniture and no one in this room was harmed during the attack. The door to another room was held shut allowing many of the room’s occupants the time to jump out the window, potentially avoiding being shot. One could argue that even during this extreme situation, “hiding” was the better initial option as people who had been on the third floor

were shot when they left shelter and came down to the second floor.

An animation created by the Broward County Sheriff's Office utilizing the CCTV from within the Marjory Stoneman Douglas High School in Parkland, Florida shows the movements of attacker Nikolas Cruz as he killed seventeen people in the worst school shooting at a U.S. high school. Cruz never once actually entered a single classroom. His initial attack focused on the first floor and occurred without warning to staff or students within the building. The use of an assault rifle provided Cruz with the ability to rapidly shoot people both in the hallways and through classroom doors while people inside were still exposed in these classrooms and visible from the hallway. Students and staff on the second floor apparently heard the gunshots and implemented a traditional lock down configuration; however students and staff members on the third floor heard and reacted to the fire alarm which had been triggered by smoke created by the gunfire. As Cruz transitioned from the first floor to the second, students sheltered in their classrooms were not harmed; however it was entirely different when he arrived on the third floor. Those who were caught reacting to the fire alarm by trying to evacuate the building were easy prey and more carnage occurred on the third floor. It is reported that Cruz also attempted to shoot people fleeing outside the building by firing through a window, however these attempts were thwarted due to the robust hurricane rated glazing in the school's windows.

Fight or flight response is a physiological reaction to those facing a perceived harmful event or an attack. Therefore running as a first option may seem natural, while sheltering may seem counterintuitive. Running when immediately threatened, such as when exposed outside of a classroom or while in a large gathering area that has been penetrated by an attacker is a prudent action to avoid harm, just like moving out of the way of a moving vehicle would be wise. However, remaining within a locked classroom while in a traditional lock down configuration has proven time and again to be a valid strategy to avoid harm during a school shooting. Therefore universally applying the Run, Hide, Fight strategy as it was initially proposed by the City of Houston to the school environment, may be imprudent and dangerous for students and staff.

Classrooms often provide a known safe environment. Attempting to evacuate students during an attack, especially in large multi-storied building, without certain knowledge where the attacker is located or if the route to the outside is safe could likely have deadly consequences. Encountering an armed attacker in a stairwell, for example, could have dire results. The uncertain atmosphere during an attack does not ensure that the exterior of the building is significantly safer. Attacks have occurred at school facilities employing improvised explosive devices, sniper type tactics and vehicle ramming. The prospect of an uncontrolled mass and chaotic evacuation would also make any law enforcement response daunting. Moving students who are separately sheltered in classrooms together in large groups outside the building has the potential to create the precise situation that a mass killer would desire to maximize carnage. Far too often the attacker is a member of the school community who would have inside knowledge of the safety plan, thereby enabling the attacker to exploit a mass evacuation during an attack.

While each school building and community is unique, law enforcement professionals who provide guidance to their local school facilities should research past events and recommend proven, evidence based strategies to improve safety. There is simply too much at stake.





# Why Leaders Lose Good People



**H**ow do you first react when employees quit? Do you think, *They're foolish for leaving? It's best for them?* As they clean out their desk, remember that 1) personnel do not usually change jobs solely for money and 2) they unlikely resign on a whim or in a fit of anger. People joined your organization because they considered it right for themselves at the time, and it probably was. So, what transpired between the day you hired them and the day they quit?

## ABSENCE OF LEADERSHIP

Personnel need effective, trustworthy leadership. Without it, they will struggle to perform at their full potential. Employees' productivity may slip if their leaders do not provide proper direction regarding the organization's vision and goals. In addition, without needed support employees more likely will become frustrated and discouraged and lose their motivation to devote their full effort to the job. Lack of leadership can result in lowered productivity, wasted time and resources, diminished morale, and increased turnover.

## LACK OF ORGANIZATIONAL VISION

An agency without a clear vision statement—a roadmap—allows for too much speculation. Without this direction, employees must wait to see what happens next. They less likely will understand the organization's overall expectations and objectives, let alone their own roles.

Personnel want to know what they are striving for and how their efforts fit within the agency. A vision statement allows them to think creatively and take initiative, rather than simply wait for assignments. As a result, they feel free to work independently within the confines of the vision.

Further, employees emotionally attached to the vision believe in what they do and become more committed to the organization. They consider their job important.

## MICROMANAGEMENT

When monitored too closely, employees feel that they have no independence. Micromanagement causes personnel to lose the desire to do anything other than what leaders want them to do and nothing more. No one "steps outside the box" or puts in extra work when micromanaged. Employees' skills will diminish, leaving the agency with personnel who know how to do only what they are told. Such an environment results in individuals who lack innovation, depend on direction, distrust management, and want to leave.

## FAILURE TO DEVELOP PERSONNEL

Neglecting to build employees' skill sets can devastate their morale. Developing and growing personnel helps eliminate their desire to look outside the agency for promotion. When trained and mentored, individuals understand the organization from the inside out. They become competent and independent both now and in the long term. Further, when leaders promote from within, employees see that advancement opportunities exist within the organization; this leads to higher productivity and morale.

## FOCUS ON THE WRONG PEOPLE

Through employee development, agencies discover their best performers. Leaders must identify the organization's top personnel—the ones worth investing in who will, in turn, give their time and energy to the agency. It is critical to offer opportunities to the employees who deserve them; they put more value in the future than the present.

Agencies must promote only ideal candidates. To this end, a well-trained team provides a deep internal hiring pool from which to select during a promotion process. Leaders who consistently develop and promote their employees lead their organization into the future with a clear and coherent vision.

Capable, hardworking personnel want to work with others who share the same work ethic and perform optimally. When leaders fail to properly evaluate candidates and to hire the best, it can demotivate those stuck working alongside them.

Promoting the wrong personnel can prove devastating. When employees "go the extra mile" and put in additional work only to lose out on a promotion to someone who received it because of deception or favor, it is an insult. Such action often makes good people leave.

## TOXIC EMPLOYEES

Personnel who continue exhibiting destructive behaviors, such as anger, laziness, or incompetence, can ruin the performance of a team or an entire organization, regardless of how effective other employees are. Such behaviors are remarkably contagious. Agencies that hire or continue to retain such personnel allow them to become toxic and subsequently set the stage for the most skilled employees to fail. Leaders must do all they can to screen individuals before hiring them. If people with concerns slip through, organizations must make every effort to reform or, if necessary, get rid of them.

## CONCLUSION

Losing good people negatively impacts employee morale and productivity. Recruiting and training new personnel require time and money, and staff members must carry the extra workload. Further, when honest, capable employees leave, they often take a wealth of knowledge and experience with them.

Agencies must retain such personnel. Leaders need to guide their organization according to its mission and vision statement. They must develop employees without micromanaging them. Further, leaders need to identify, hire, and promote ideal employees while getting rid of poor ones. Keeping good people is easier than replacing them.

*Reprinted with the approval of the FBI Law Enforcement Bulletin. Undersheriff Vernon Knuckles of the Montezuma County, Colorado Sheriff's Office prepared this article. He can be reached at [knuckles67@google-mail.com](mailto:knuckles67@google-mail.com).*



# Confronting Terrorism in New York State

BY: ROBERT GARDNER  
SENIOR INVESTIGATOR OF THE NEW YORK STATE POLICE

New York State remains a top target for terrorism and deserves the highest levels of protection. It is considered the #1 target for terrorists since it is the iconic symbol for freedom as well as the financial capital of the country. Since 9/11, in New York City and throughout New York State there has been several terrorism investigations that have either stopped potential attacks or prevented aiding a Foreign Terrorist Organization (FTO).

Terrorism has evolved from the terrorism cell targeting multiple targets to the individual Homegrown Violent Extremist (HVE) who

**Both HVE and Domestic Extremists communicate via social media “Free Messenger” applications such as Rocket, Viber and Discord thereby avoiding detection by law enforcement.**

is self-radicalizing at their residence anywhere in the United States. Often times the HVE has never left the country and is a citizen of the United States. This presents challenges for law enforcement to combat terrorism in this country on many different levels. There are two critical challenges for terrorism investigations. They are: The identification of the HVE based on suspicious patterns using intelligence led policing; and interrupting the terrorist plan and the furtherance of the “terrorist cycle”.

## HVE AND DOMESTIC EXTREMISTS

HVE and Domestic Extremists are two different sets of terrorist groups with distinct target selection practices driven by specific grievances based on their respective ideology. Domestic Extremists respond swiftly with violence to socially and politically charged events in the U.S. A HVE is a person of any citizenship who has mostly lived in the U.S. and who engages in a terrorist activity to advance an ideology. This person is influenced by foreign terrorist organizations but acts alone and is generally not in contact with an “official” from the foreign terrorist organization. Often times the radicalization does not involve the extremist having any in-person contact with a radicalized member. The radicalization process includes online materials consistent with violent extremist narratives, which contribute to their radicalization processes. Both HVE and Domestic Extremists communicate via social media “Free Messenger” applications such as Rocket, Viber and Discord thereby avoiding detection by law enforcement. Another growing form of messaging is via the gaming platforms and the individual applications available on that platform such as “Fortnite”. Once the HVE self-radicalizes, the target selection is based upon the specific grievances promoted by each attacker’s respective ideology. Target selection may include a broad range of civilian and government-related locations. Recent cases in the United States show that mass gatherings and religious institutions were the primary targets by HVE and Domestic Extremist. These target sets may be attacked using by conventional or unconventional weapons such as explosives, weapons or vehicles.

## OPERATION SAFEGUARD

Some of the tools being used in New York State to assist law enforcement and prevent the mobilization of terrorism is under

the Operation Safeguard umbrella called the “See Something Say Something” program. This program encourages all New Yorkers to report suspicious activity to any law enforcement agency or to the New York State Terrorism Tips Hotline (866-Safe-NYS) housed at the New York State Intelligence Center (NYSIC). NYSIC personnel will document and analyze any information received and notify the appropriate law enforcement agency.

## THE RED TEAM PROGRAM

The RED TEAM Program is another tool used in New York State parallels the “See Something Say Something” program. The program is used as an educational tool that is spearheaded by the New York State Department of Homeland Security and Emergency Services (NYSDHSES).



***Purchases made during a Red Team exercise to imitate a suspicious purchase.***

The Red Team program is employed across the state and has been so successful that other states have expressed interest in copying the program. A Red Team exercise is designed to test a location, business or government entity unannounced and monitor their reaction to the

test. The hope is that once suspicious Red Team activity is detected, the people at the tested location will promptly report said activity to law enforcement. Acceptable methods of reporting include reports made via telephone (911 or regular police phone numbers), the Terrorism tips hotline, walk-in reporting at a police station, and notification to a relative or friend that is in law enforcement.

The Red Team program uses members of the FBI's Joint Terrorism Task Force, New York State Police, county sheriffs, and police departments partnered with the state's Office of Counter Terrorism personnel to plan and execute Red Team exercises. In total, nearly 100 law enforcement agencies and 300 personnel across the 16 Counter Terrorism Zones participate in the program. This year about 1000 locations were tested by nearly 100 law enforcement agencies and 350 personnel. Tested locations included:

- 100 truck rental locations;
- 5 upstate airports;
- Hardware and gun stores;
- Large retailers;
- Vehicle rental locations;
- Businesses that sell chemicals or components used in the construction of improvised explosive devices;
- Hospitals, colleges and universities;
- Transportation infrastructure;
- Drone dealers;
- Mass gathering sites and other locations that could be targeted by terrorists.

At each location, law enforcement personnel tested security protocols by engaging in "suspicious activity". For example, Red Team personnel would inquire about various chemicals and components used in improvised explosive devices. The business response to this nefarious activity would then be monitored to determine if their employees would notify law enforcement. After

each visit, federal, state, and local homeland security agencies would meet with the personnel of the tested location to point out successful activity as well as identify areas of improvement. In most instances, the activity was reported promptly and accurately. However, when activity was not reported, follow up education by team members was well received.

Each of the locations tested and their contact information are documented in the Operation Safeguard database and accessible to law enforcement. The Red Team exercise reflects a reporting average of 34% in 2018 compared to 26% in 2016. This increase in reporting illustrates the value and success of the Red Team program and is very encouraging because the ultimate mission of Red Team is twofold: First, to build a general public awareness of terroristic suspicious activity and second, how to report that activity. A gauge of the Red Team exercises success is that reporting of actual tips of suspicious activity has increased dramatically leading to viable counter terrorism investigations that have resulted in arrests and prosecution.

Terrorism will always present a challenge for law enforcement and since detection is becoming harder, these tools are invaluable. Operation Safeguard is the new form of Community Policing designed to build relationships with businesses and community members so that intelligence led policing can bridge the communication gap and assist in the overall mission of counter terrorism.

*Senior Investigator Robert Gardner is a 25 year member of the New York State Police and is the Supervisor of the Counter Terrorism Intelligence Unit - Western Region of New York State. He is a graduate of Hilbert College and holds a Master Degree in Criminal Justice Administration from Hilbert College.*

*Email – [robert.gardner@troopers.ny.gov](mailto:robert.gardner@troopers.ny.gov)*

# Bulletproof Vest Partnership: What You Need to Know to Receive Federal Funds

Picture Courtesy of Gauls Event



## HISTORY

Created in 1998, the Bulletproof Vest Partnership (BVP) is a grant initiative program of the U.S. Department of Justice (DOJ) administered by its Bureau of Justice Assistance (BJA) arm in conjunction with state and local law enforcement to help supplement the purchase of bulletproof vests for their officers. With preference towards small town America, federal funds are allocated first to

jurisdictions with less than 100,000 residents.

In its current iteration, the Bulletproof Vest Partnership Grant Program Reauthorization Act of 2015, via the 114th Congress, extends appropriations for the BVP program annually through fiscal year 2020.

## FACTS

Since 1999, more than 13,000 jurisdictions have been awarded almost \$450 million in federal funds (as of March 2018) for the purchase of over 1.3 million protective vests for their officers. This average's to over \$34,000 per jurisdiction in matching funds. The program is designed to cover upwards of 50% of eligible vest costs and has proven to be the difference between life and death for many officers across America.

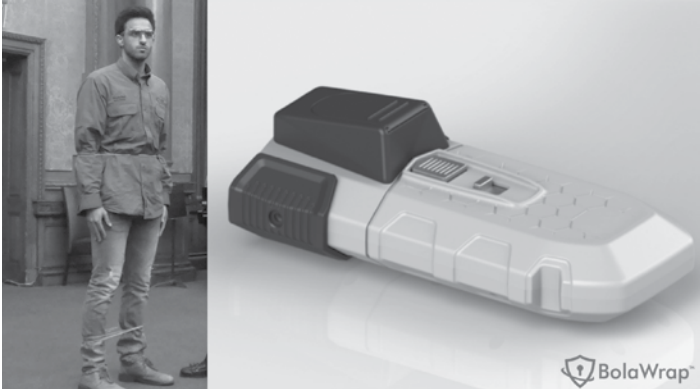
## THINGS TO KNOW

- Only law enforcement officers may receive vests through the program (full-time, part-time, paid or volunteer; officers in academy are eligible).
- Vests must meet the most current National Institute of Justice (NIJ) standards.
- One vest per officer in a replacement cycle (usually 4-5 years).



# Technology Update

**B**olaWrap by Wrap Technologies is a new law enforcement product that recently came on the market and is being tested by police departments across the country. The handheld



BolaWrap 100 is a remote restraint device that discharges an eight-foot bola style tether at 640 feet per second to entangle a subject's extremities at a range of 10-25 feet. The manufacturer states that BolaWrap ensures a safe space between the Police Officer and their subject, does not rely on pain compliance, and is specifically

designed to be deployed early in an engagement. It is designed for the non-compliant or the mentally ill population where other law enforcement tools are not effective or appropriate. The device can be worn on the duty belt, carried in a pocket, or affixed to the outer carrier of a vest.

Yonkers PD is currently testing BolaWrap. According to Yonkers Police Commissioner Charles Gardner, their training unit is in the



—*TECHNOLOGY UPDATE, continued on page 22*

- **Mandatory Wear Requirement:** This is intended to ensure that the body armor procured with BVP funds appropriated by Congress is worn by law enforcement officers to reduce line-of-duty deaths. A written mandatory wear policy must be in effect at the time the jurisdiction submits its application for BVP funds (policy will be subject to random review and verification to include, but not limited to, the date it was first implemented). This written policy must remain in effect for the life cycle of the vests purchased with BVP program funds. Any subsequent modifications in the policy must be submitted to the BVP program for a complete compliance review. Agencies via its Chief/Commander have the authority to grant exceptions for individuals, assignments, organizational units, climate-related situations and other factors as determined at the local level, including medical considerations. A copy of a sample model policy, **Body Armor Model Policy and Issues Paper**, can be obtained by contacting the BVP Help Desk at 1-877-758-3787 or by email at [vests@usdoj.gov](mailto:vests@usdoj.gov).
- **Uniquely Fitted Vest Requirement:** the BVP Reauthorization Act of 2015 provides that a preference be given to BVP grant recipients for body armor that is uniquely fitted, particularly that which is applicable to individual female law enforcement officers. Uniquely fitted means protective vests that conform to the individual to provide the best possible fit and coverage through a combination of: 1) correctly-sized carriers and ballistic panels as appropriated measured, and 2) properly adjusted straps, harnesses, fasteners, flaps or other adjustable features. "Uniquely fitted" does not necessarily require that the respective vest be individually manufactured based on the physical measurements of the individual wearer. Beginning with the 2018 BVP program application, a certification section has been added that jurisdictions and agencies applying for BVP grant monies must state that they are aware of and will comply with this fitted vest requirement.
- Tactical vests are eligible, but it must be that officer's primary vest.
- Only one BVP application per jurisdiction per program year

(additional vests may be applied for in subsequent years; annual 6-week application period usually begins in April).

- BVP funds generally become available 3-4 months after the application deadline (notification will be via email, roughly late summer).
- Vest changes can be made after the application has been submitted (BJA recognizes operational and equipment needs may change since the date of application submission).
- Other federal funding, such as Justice Assistance Grants (JAG), may not be used to cover any balances not provided for by BVP funds.
- Vests for K9's are currently ineligible.
- Helmets & shields are currently ineligible.
- Hardship waivers are available and provide jurisdictions in financial hardship the ability to request up to 100% of the cost of each vest to be covered by the BVP grant (certain criteria apply).

## RELEVANT INFORMATION

- BVP Site: <https://ojp.gov/bvpbasi/>;
- BVP User Guides and Checklists: (can be found under "Program Resources" in the above link);
- BVP Grant Registration/Application: (can be found under "Login" in the above link).

## APPLICATION PERIOD

Annual 6-week application period usually opens in April, ending in May (Apr 12 - May 29, 2018; May 17 - Jun 28, 2017; Apr 4 - May 16, 2016; Apr 1 - May 13, 2015).

If you wish to be contacted when this year's application period has been announced, please contact me:

By Michael Schiller - Tactical Supply Group  
[mschiller@tacticalsupplygroup.com](mailto:mschiller@tacticalsupplygroup.com)  
[tacticalsupplygroup.com](http://tacticalsupplygroup.com)  
718-313-1979



initial stages of evaluating the effectiveness and possible uses for BolaWrap. Commissioner Gardner was generally impressed by the product along with the availability of providing an additional less-lethal option for his officers. The YPD is also researching the drafting of a policy to address the use of BolaWrap.

The Chiefs Chronicle magazine attempts to keep our membership informed of new products that may be of interest to the New York State law enforcement community. These informational articles are based on news articles and news releases supplied by manufacturers and distributors. The articles are in no fashion an endorsement of any product by the NYSACOP.



# Strategic Planning for Small Law Enforcement Agencies

Smaller law enforcement agencies often face an uphill battle due to limited resources

BY: CHIEF JONATHAN B. FLORES, P1 CONTRIBUTOR

The law enforcement profession is fluid and police leaders must be able to forecast emerging trends that will allow them to plan strategically for the future of their department. Over the years this has become increasingly difficult as the economy becomes more unpredictable.

Strategic planning for any law enforcement entity serves as a document that provides the vision and goals of the organization over time,

Smaller law enforcement agencies often face an uphill battle due to limited resources and competitive grant opportunities that require an unattainable match. These agencies still need to provide the same quality service to their communities as any other mid- to large-size agency; however, they must do more with less.

Strategic planning for any law enforcement entity serves as a document that provides the vision and goals of the organization over time, with a roadmap for how those vision and goals will be accomplished. For a smaller organization a strategic plan provides stakeholders with a living document that allows for proper planning toward the priorities of the organization in accordance with the operating budget. The following steps can help create a strategic plan for your agency.

## 1. Set a clear vision and goals

LE leaders must be able to set a clear vision for their agency, so everyone knows the plan for the organization. Once a clear vision has been set, goals should be established, along with a time frame for accomplishing those goals.

## 2. Forecast your budget

It is a good rule of thumb to increase line items by at least 15 percent when forecasting future budgets. Certain line items such as fuel can be very unpredictable, so you should compare your previous fuel budget and allow for increases. It is always better to forecast a higher number and come under budget.

## 3. Prioritize your goals

When creating a strategic plan, consider goals that can be achieved with minimal impact to the budget (low-hanging fruit). Such quick victories will boost morale within your organization and make an impact within your community. These items can be accomplished while allowing time to achieve more lofty goals that require a more significant investment.

## 4. Set reasonable time frames

A three- to five-year strategic plan allows enough time to implement thorough, effective measures to achieve the vision and goals of the strategic plan.

## STRATEGIC PLANNING IN PRACTICE

Using the steps above, my department – which is comprised of 21 sworn officers and six civilian staff – created the following strategic plan:

### Short-range goals

One short-term goal for the Alton Police Department was to re-brand the agency via new vehicle decals, new uniforms and new patches. (*Photo/Chief Flores*)

All these items had a minimal impact on our operating budget, but they had a huge impact on morale and our community's perception of our department:

- Re-branded our agency via new decals for our units, new uniforms and new patches.
- Created a social media page to allow us to be more accessible and transparent to our community.
- Organized community events such as Alton's first annual National Night Out.

### Mid-range goals

We understood that while larger ticket items were a priority, they would take a little more time to accomplish.

- We reviewed our operating budget and allotted ourselves six months to acquire a CAD/RMS system for our communications center. This item took time, planning and support from our city administration to acquire. After going through these steps, we were able to acquire the system that improved the efficiency and effectiveness of our department within four months of our six-month goal.
- We implemented a bike patrol program within four months of our one-year goal that required investments in equipment and training, however the impact that this program has made in our community has already paid dividends.

### Long-term goals

We continue to work toward increasing department personnel in our communications center, patrol and investigations divisions in order to serve our growing community with the highest level of service. We understand that this part of our strategic plan will take the longest and must be done in increments over time to ensure a smooth transition in our operating budget.

I have found much success in strategic planning for my organization. My hope is that this article will assist those in similar situations to improve the efficiency and effectiveness of their organizations via a solid strategic plan.

## About the author

Jonathan B. Flores is chief of police for the Alton (Texas) Police Department. Chief Flores is a former homicide investigator for the Hidalgo County Sheriff's Office and has 16 years of law enforcement experience. He has a Master's Degree in Public Administration from the University of Texas Rio Grande Valley and a Bachelor's of Science in Criminal Justice Degree from the University of Phoenix.







# WE SALUTE YOU

## Capital Cardiology Associates

On behalf of the 20 shareholder  
cardiologists of:

Dr. Augustin DeLago, MD, FACC, FSCAI  
PRESIDENT AND CEO

## THANK YOU FOR YOUR SERVICE

[www.CapitalCardiology.com](http://www.CapitalCardiology.com)



# The **VALUE** of **PATIENCE** **UNDER STRESS!**



NEW YORK STATE ASSOCIATION  
OF CHIEFS OF POLICE, INC.  
24 Century Hill Drive  
Latham, New York 12110

—SAVE THE DATE—

NEW YORK STATE ASSOCIATION OF CHIEFS OF POLICE

—SAVE THE DATE—



ANNUAL TRAINING CONFERENCE  
JULY 21 - JULY 24, 2019



HYATT REGENCY ROCHESTER  
125 EAST MAIN STREET  
ROCHESTER, NEW YORK



**Keeler**  
MOTOR CAR COMPANY



Keeler Motor Car Company is a  
proud sponsor of The NYS  
Association of Chiefs of Police



SPRINTER  
METRIS

**Keeler**  
Pre-Owned

KEELER MOTOR CAR COMPANY  
**COLLISION**  
Center

Route 7, Latham, NY • (518) 785-4197  
Visit us online at [www.keeler.com](http://www.keeler.com)