

*The opinions expressed in this newsletter are those of the author's and do not reflect the views of LGRMS, ACCG, or GMA.*

THE WHY, THE WHAT, AND THE HOW:

# CYBER & SOCIAL ENGINEERING

P.4

ALSO IN THIS ISSUE  
MITIGATING STRESS  
REACTION & SUN SAFETY

## SAFETY THEME

DOWNLOAD THIS MONTH'S  
SAFETY POSTER

## HEALTH PROMOTION SERVICES

CHECK OUT THE LIVING WELL  
GEORGIA CORNER

## RISK/LIABILITY

NOTES FROM THE ROAD AND  
OTHER GREAT ARTICLES

# CONTENTS

- 3 A Note from the Editor  
New Publication Format and Name Change
- 4 Director's Corner  
Cyber & Social Engineering
- 15 Liability Beat  
Immunity for Officer
- 25 Mitigating Stress Reaction
- 28 Notes from the Road  
Reopening the State
- 29 American Policing  
Strategies and Tactics
- 26 Fun With Safety  
Word Search/Crossword Puzzle
- 33 HPS - Living Well Georgia  
Sun Safety, Going Back Out, & a Forum Call
- 36 Safety Theme  
Insect Hazards - Ticks
- 39 Safety Forms  
General Safety Inspection Form/Attendance
- 42 LGRMS Contacts
- 43 Special Announcements



3500 Parkway Lane  
Suite 110  
Peachtree Corners, GA 30092

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

## UPCOMING WEBINARS AND TRAINING EVENTS

For a current list of training events, please visit:

[www.lgrms.com/trainingcalendar](http://www.lgrms.com/trainingcalendar)

### **ACCG and GMA Workers Compensation Webinar**

Tuesday, JUN 22, 2021 // 10:00am - 12:00pm

### **ACCG and GMA Workers Compensation Webinar**

Tuesday, JUN 24, 2021 // 1:00pm - 3:00pm

This webinar is targeted toward City and County administrative staff who oversee the Workers Compensation program for their local government, elected officials who want to know the fundamentals of how the program works, and supervisors of employees.

Please log into the [LGRMS Website/training calendar](http://www.lgrms.com/trainingcalendar) for a complete list of training events.



# A NOTE FROM THE EDITOR

By Dennis Watts,  
LGRMS Training, Communication, and Public Safety Risk Manager

## New Publication Format and Name Change

Welcome to the fifth edition of SHARE, the new combined monthly publication of Local Government Risk Management Services (LGRMS). SHARE is sent to all GIRMA/IRMA, WC, and Life & Health members 10 times per year (June/July and November/December issues will be combined).

SHARE will have two sections: (1) a general safety, risk, and health section, and (2) a worker safety-focused section similar to the old Safety Theme.

We cover those topics and issues most relevant to Local Governments in Georgia, plus some new features. We look forward to your feedback. The LGRMS SHARE is published on or around the 20th of each month. If you are not currently on the distribution list to receive our monthly newsletter, it can be downloaded for free from the LGRMS website ([www.lgrms.com](http://www.lgrms.com)).

### In this issue

Welcome to May SHARE. In this issue we have a variety of articles focusing on current topics affecting local governments. Workers and worker safety is always our number one focus. Our employees are our greatest asset. Supporting this, we have several articles: for outdoor workers, a safety theme focused on managing and avoiding

ticks, and a great article on sun safety. This issue also covers the why and how of cyber and social engineering. Local governments are particularly vulnerable to these attacks. Awareness and training are the keys to preventing them.

Should you have any questions or concerns, please contact: Dennis Watts, [dwatts@lgrms.com](mailto:dwatts@lgrms.com), or

Tammy Chapman, [tchapman@lgrms.com](mailto:tchapman@lgrms.com).



# DIRECTOR'S CORNER



By Dan Beck, LGRMS Director

## THE WHY, THE WHAT, AND THE HOW: CYBER AND SOCIAL ENGINEERING

### The Why

Cyber and social engineering losses are on the rise, both in frequency and in cost. In 2020, Twitter, Zoom, Magellan Health, Marriott International, and MGM Resorts suffered some of the largest known data breaches to-date. Rob Sobers' list of 11 Impactful Cybersecurity Facts and Stats illustrates some of the

recent trends and impacts of cyberattacks and social engineering claims.

1. 95% of cybersecurity breaches are caused by human error. (Cybint)
2. The worldwide information security market is forecast to reach \$170.4 billion in 2022. (Gartner)
3. 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
4. 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
5. On average, only 5% of companies' folders are properly protected. (Varonis)



6. Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
7. 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
8. 45% of breaches featured hacking, 17% involved malware, and 22% involved phishing. (Verizon)
9. Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (ID Theft Resource Center)
10. The top malicious email attachment types are .doc and .dot, which make up 37%. The next highest is .exe at 19.5%. (Symantec)
11. An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)

A significant number of large cyber incidents have occurred within local governments across the country. As you can see from the chart\$ below, the ransom demands are rising.

These types of claims have also been reported by several Georgia city and county members to the property & liability insurance pools sponsored by the Georgia Municipal Association (GMA) and the Association County Commissioners of Georgia (ACCG). All events required thousands, if not hundreds of thousands of dollars, in event management and mitigation expenses.

In addition to cyber breach events, there is a growing prevalence of social engineering losses. Social engineering losses occur when manipulative tactics



LOCAL GOVERNMENT	DATE	RANSOM DEMAND	ESTIMATED COST
Atlanta, GA	Mar-18	\$51,000	\$17,000,000
Baltimore, MD	Jul-19	\$80,000	\$6,000,000
New Bedford, MA	Jul-19	\$5,300,000	Not reported
Pensacola, FL	Dec-19	\$1,000,000	Not reported
Wilmer, TX	Aug-19	\$2,500,000	Not reported

\$Based on different articles

are used to trick someone into giving up confidential information. The most common social engineering losses currently being seen by members of the GMA and ACCG pools are related to invoice manipulation. One member suffered two separate fraudulent wire transfer claims of \$98,320 and \$393,280. Other members suffered similar fraudulent wire transfer claims in the amounts of \$800,000 and \$150,000. Details on how these incidents occurred will be provided later in the article.

You might say, well it's good we have insurance. The bad news is insurance may not cover some of these losses due to exclusions and/or sublimits.

Lindsey Albright, GMA's property & liability pool's Account Executive from Willis Towers Watson, writes "Cyber insurance coverage offers protection for four main areas as follows:

- (1) Security & Privacy Liability- Responds to third party liability claims arising out of:
  - a. A failure of the Member's network security
  - b. A failure to protect personally identifiable information from misappropriation, including disclosures as a result of social engineering attacks (e.g., phishing)
  - c. A failure to protect or wrongful disclosure of private or confidential information
  - d. Violation of any federal, state or local privacy statute alleged in connection with failure to protect private information
  - e. Broader definition of "computer system" to include leased computers

- (2) Event Management Coverage- Responds to the costs to retain public relations services to assist in managing and mitigating a covered privacy or network security incident.
  - a. Includes costs to notify consumers of a release of private information. Such notification is now mandated by most states and can be very costly
  - b. Includes cost of credit-monitoring or other remediation services to help minimize damages to those victimized by a covered privacy or network security incident
  - c. Includes costs associated with losses to information assets such as customer databases resulting from a failure of network security
  - d. Provides vital protection for "intangible"





assets that are not covered by traditional property insurance

- (3) Extortion- Coverage responds to the threat of intentional security attacks against a member by an outsider attempting to extort money, securities, or other valuables. This includes monies paid to end the threat and the cost of an investigation to determine the cause of the threat.
  - a. Includes Legal Expenses
  - b. Includes the costs of forensics to recover or rebuild data
  - c. Includes costs associated with Extortion/Ransom payment (with carrier consent)
  - d. Includes access to bitcoin or cryptocurrency, as needed
- (4) Social Engineering\*- Responds to fraudulent electronic, telegraphic, cable, teletype or telephone instructions issued to the insured

directing the insured to debit a Transfer Account and to transfer, pay or deliver Funds from such Transfer Account through instructions which have been transmitted by someone purporting to be an authorized employee or outsourced provider of the insured.

*\*The ACCG property & liability insurance pool provides Social Engineering coverage under the Crime Section of the Coverage Agreement.*

Cyber coverage for all insureds, but specifically public entities, is becoming increasingly more expensive and more challenging to purchase in general. Public entities are a primary target of cyber criminals. The cost of coverage is increasing exponentially and the amount of coverage available is becoming more and more limited as capacity shrinks. Insurance carriers

# CYBER LIABILITY

## State of the Market and claims, legal, emerging trends

### Rate Prediction: +30% to >50%

- Cybercriminals are targeting businesses of all kinds with ransomware attacks. As these attacks become more sophisticated, carrying the potential to effect a wholesale inability to access a firm's entire electronic infrastructure, ransom demands have increased — often reaching eight figures.
- This explosion in severity, coupled with high frequency, has had a direct impact on premiums, capacity and underwriting scrutiny.
- Carrier strategy revolves around obtaining adequate premium for perceived risk. There is less aggressive competition, especially where security measures are considered lacking or pricing is "too thin."
- Insurers are partnering with third parties, such as BitSight and Security Scorecard, to identify insured's externally visible cybersecurity vulnerabilities. Carriers may require certain vulnerabilities be addressed prior to quoting.

**\$1mil**

Typical ransomware loss in 2019

**\$3.86 mil**

The average cost of a data breach in 2020 is \$3.86 million, according to a new report from IBM and the Ponemon Institute.

**63%**

Cyber losses attributable to the human element

are dropping out of the cyber space because it is not a profitable line of business. Public entities will likely need to take higher deductibles and pay higher premiums to obtain the coverage.

Here is a recent state of the market from our cyber group:”

## Cyberattacks

### The What, How They Attack, and How We Control

#### The What

Merriam-Webster<sup>3</sup> defines a cyberattack as: an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.

This damage or harm can result from a wide range of tactics:

- Ransom – As discussed in the previous incidents, the attackers infect your systems with a software or malware. Malware allows the attackers to shut down your system in an effort to prevent you from accessing data until the ransom is paid.
- Information & Financial theft – With this tactic, you might not even know someone has hacked your system. The attackers may steal the financial data of others, credit cards numbers, social security numbers, etc. The hackers might want to steal directly from your customers or just access your business’ financial systems to steal directly from you.

- Business interruption, vandalism, or terrorism – As in the famous film War Games, hackers may enter your systems just to see what they can do. As in the February 2021 Florida water treatment facility hack, they accessed software with the intent to poison customers.
- Reputation theft – Of all these tactics, the loss of reputation and trust is typically the most damaging.

#### How They Attack

Cyberattacks take many forms, but we will focus on the three below.

- Your Password
- Phishing, Spear-phishing, Smishing
- USB Attack

#### How Hackers Use Your Password to Conduct Cyberattacks

There are a variety of ways someone can use your password to gain access to your system.

- Trial and Error – Many of us use very simple passwords. If you do an internet search for common passwords, you will find that “password” is typically in the top 10. Hackers utilize software that systematically tests password after password until the correct password is identified.
- Educated Guess – Many hackers use social media and other means to find names for your children or pets, or special dates in your life. These names and numbers are commonly used because they are easy to remember.



- Your Password –
  - o Some of you write down your password and store it someplace handy (e.g., sticky note on the computer, or under the keyboard, or on the shelf). If a hacker walks by your desk, you have just made it very easy for them to access your accounts.
  - o If a hacker is watching you type your password, a talented hacker may be able to memorize your keystrokes.
  - o If a hacker already has access to your system, they may be able to see your password from a remote location as you type it.

The below graphic from “HowSecureisMyPassword.net” shows how long it takes to crack passwords of various complexity. As you can see, the longer and more complex your password is, the more secure it is. It is important to remember that these are minimum requirements. This time chart assumes that a hacker can try passwords as often as they like.

## TIME IT TAKES A HACKER TO BRUTE FORCE A PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

## How You Can Protect Against Hackers Using Your Password

- Use complex passwords – Use a multiword phrase you can remember, or use a combination of numbers, special characters, and lower-upper case alphabets. Avoid using special well-known names or dates.
- Set a limit on the number of login attempts.
- Memorize your passwords or use a verified password protection program like LastPass.
- Don't write your passwords down for others to see.
- Don't allow people to watch your keyboard when entering your password.
- Never share your passwords, even with your IT group.
- Always blank or block out your password on the screen when typing.
- Use multi-factor authentication – this requires a code or confirmation from a text message or other delivery mechanism.

## How Hackers Use Phishing, Spear-phishing, Smishing to Conduct Cyberattacks

Within the practices of phishing, spear-phishing, and smishing, a hacker typically sends an electronic message from a seemingly trusted source. Their goal is to lure you into clicking a link or opening an attachment. As stated previously, once you click on those items, malware is loaded onto your system.

Phishing emails are more generic and have widespread distribution. These emails might send you a picture, file, or link that most people would find interesting.

Spear-phishing focuses on specific individuals. Hackers do research via social media or company websites to identify language or tasks that you might typically see in work-related emails. For example, a hacker could research that you are in safety and risk management and send you a link to a safety video, or identify a coworker and fake an email from them.

Smishing is similar to phishing, but involves a malicious text message as opposed to an email.

### **How You Can Protect Against Hackers Using Phishing, Spear-phishing or Smishing**

- Check the specific email address of the sender. Even though you might recognize the name, the email might be fake. There are 3 parts of an email address: username@domain. The last part of an email address is the domain, which can be broken down into two portions: the mail server and the top-level domain (.com, .net, .org, etc.). If the domain portion of the email address doesn't match others within that organization, it may be a hacker. Hackers often change one letter in the domain name to trick recipients.
- Don't click on links or open attachments sent from unknown sources.
- When in doubt, pick up the phone and call the sender. If they don't have a phone number, it is likely a hacker.
- Report all potential phishing, spearfishing, and smishing emails to your IT professional.

### **How Hackers Use USBs, Thumb Drives, or CDs To Conduct Cyberattacks**

Have you ever found an old USB or thumb drive laying around and asked yourself what is on it? That is the thought process hackers are relying on. So, they will give them to you, place them in your drawer, on your desk or leave in a conspicuous place to be found. They may label them with provocative phrases like "Top Secret", "For Your Eyes Only", or "Holiday Pictures" in order to lure you into plugging them into your system. Once you plug them in, the malware is loaded into your system.

### **How You Can Protect Against Hackers Using USB, Thumb Drives, or CDs**

- Only use secure and trusted USB devices, thumb drives, or CDs. These should be cleared for use by your IT professional prior to use.
- If you don't recognize the USB, thumb drive or CD, don't use it. If you want to find out what is on a found device, contact your IT professional. It is never advisable to use an unknown storage device in your work environment.

## **Social Engineering**

### **The What, How They Attack, and How We Control**

#### **The What**

Social engineering hackers use psychology to exploit or manipulate human targets rather than technology. Hackers assume you want to do a good job, you want to



please your bosses or customers, and you likely have too much on your plate. So, these con-artists/hackers will send you emails, texts, or phone calls with deceptive instructions or requests. They may request:

- Access to controlled areas, including physical locations and network environments.
- Personal or sensitive data, such as credit cards, bank information, or personal passwords.
- Changes to customer account information or bank routing numbers.

## How They Attack

Criminals use a variety of social engineering tactics to gain access to sensitive information or to cause harm to you or your organization.

1. Phishing – This is the most common social engineering attack. This was covered this earlier, but a criminal may use emails or malicious websites that look as if they are from a trusted source to solicit personal or protected information.
2. Pretexting – Pretexting is just what is sounds like. Criminals will give a false pretense to justify a course of action. They may create a fake identity or identify themselves as someone they are not. A fake story may be invented to fool victims into sharing valuable information to gain access to a service or system, most often to trick you out of your money. Below are just a few examples of scammers who impersonate others to trick you:
  - a. An IT professional requests that you share your password. Never share your password, even with your IT professional.

- b. Someone within your leadership team asks you to send them a list of clients, purchase gift cards, or send a check to a vendor. This is a common occurrence. Always check the last part of an email address or the domain (the mail server and the top-level domain) and call the sender by looking up their phone number. Do not trust the number included within the email.
- c. Someone posing as a contractor/vendor sends you an email requesting to switch their bank routing numbers for payment. Then, when the legitimate contractor or vendor sends you a bill, you are actually issuing payment to the criminal. This has occurred with several pool members and involved large six figure payments. See the string of actual emails below as an example.

From: Contractor / Criminal  
Sent: Friday, May 24, 2019 12:55 PM  
To: City Finance Dept  
Subject: RE: Vendor ACH/EFT Form

Hi

We are one of your construction vendors being paid by the city, do you have a vendor ACH we can use to provide our banking information?

Kind Regards,

Senior Accountant

On May 24, 2019 at 1:01 PM [REDACTED]  
[REDACTED] City Finance Dept [REDACTED] wrote:

My apologies. Are you looking to change something as we already have your information on file?

[REDACTED]

From: [REDACTED] Contractor / Criminal [REDACTED]  
Sent: Friday, May 24, 2019 1:15 PM  
To: [REDACTED] City Finance Dept [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Vendor ACH/EFT Form

2

[REDACTED]

Yes thats correct, we needed to provide our updated banking information.

Kind Regards,

[REDACTED]  
Senior Accountant

[REDACTED]

On May 24, 2019 at 1:19 PM [REDACTED] City Finance Dept [REDACTED] wrote:

Ok. If you could return the form to me as "reply all" we will get your information updated.

[REDACTED]

From: [REDACTED] Contractor / Criminal [REDACTED]  
Sent: Wednesday, June 05, 2019 2:58 PM  
To: [REDACTED] City Finance Dept [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Vendor ACH/EFT Form

Hi [REDACTED]

We were just informed the account you recently set up for us is not set up to receive ACH payments, please find attached our other account with Citibank which we have confirmed is set up for ACH payments. I have attached a voided check for accurate entry. Thanks

Kind Regards,

[REDACTED]  
Senior Accountant

[REDACTED]

From: [REDACTED] City Finance Dept [REDACTED]  
Sent: Thursday, June 6, 2019 7:58 AM  
To: [REDACTED] Contractor / Criminal [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Vendor ACH/EFT Form

Got it

[REDACTED]

3. Baiting & Quid Pro Quo Attacks – Criminals use Baiting and/or Quid Pro Quo tactics to exploit your curiosity by promising a benefit in exchange for information. They might offer you free services for music, movies, or software downloads. As discussed in the previous section, they might give you free thumb drives or CDs in exchange for revealing your password or other sensitive information. One of the most common attacks occurs when a fraudster impersonates an IT helpdesk and offers upgrades or new software.

## How You Can Protect Against Criminals Using Social Engineering Tactics

Below are few simple rules to help you protect against social engineering tactics.

- Be suspicious of every email, text, or phone call you receive.
- Slow down. While you want to be productive and have a lot of work to do, opening a malicious email or clicking a malicious link can have a serious negative impact on you and/or your organization.
- Verify, Verify, Verify
  - o Even if you think you know the person on the other end of the email, check the email address as discussed previously.
  - o If you have any questions or concerns, especially if it concerns financial, banking, or personal information, pick up the phone and give the person a call to confirm they sent the email. DO NOT use the phone number in the email. Use another source



to obtain the number such as the company website, address book, etc.

## **A Few Basic Questions for Your IT & Finance Groups**

### **How Are We Managing Our Cyber/Social Engineering Risks**

- Does our organization have a cyber security policy?
- Does our organization use anti-virus software and a firewall to protect our network?
- Does our organization do daily backups of all electronic information and data at an off-site location?
- Does our organization have a qualified person(s) or team with oversight of cyber security for all IT hardware and software?
- Does our organization provide cyber security/social engineering training to all employees with access to IT systems (password protection, phishing, and cyber security policy) at least every year?
- Does our organization have a process for testing phishing with employees?
- Does our organization use 2-factor authentication to secure remote access to our network/emails?
- If our organization sends or receives wire transfers, do we have a protocol:
  - o For obtaining proper written authorization for wire transfers?
  - o For confirming all payments or funds transfer instructions from a new vendor,

client, or customer? A direct phone call to that vendor, client, or customer is recommended. Please verify the legitimacy of the telephone number provided and do not trust a phone number listed in the email or shown on attached documents.

- o For confirming any vendor, client, or customer account information change requests, including requests to change bank account or routing numbers, contact information, or mailing addresses. A direct call to that vendor, client, or customer using only a verified legitimate telephone number should be used.

### **A Few Training Options to Assist Your Organization in Managing Cyber/Social Engineering Risks**

One of your strongest defenses against cyberattacks and social engineering risks is an effective security awareness training program. There are several vendors that provide both training and phishing email test services. If your organization does not have an outside source for this training (i.e., KnowBe4, NINJIO, eRiskHub, etc.), LGRMS provides a couple options.

1. LocalGovU – LGRMS offers all IRMA and GIRMA members access to LocalGovU's Cyber Security Course.
2. LGRMS Recently Sponsored two webinars:
  - a. Avoid The Risk Of Phishing And Social Engineering – For Staff Employees - <https://youtu.be/k2AOz8DFlyM>

- b. Avoid The Risk Of Phishing And Social Engineering – For Leadership - <https://youtu.be/5FrYKgP08wU>

## References

- 1Albright, Lindsey. (n.d.). Willis Towers Watson.
- 2Cybint, Gartner, Proofpoint, Accenture, Varonis, RiskBased, Verizon, ID Theft Resource Center, Symantec, and Cybersecurity Media as cited in Sobers, Rob. (2021). 134 Cybersecurity Statistics and Trends for 2021. From [www.varonis.com/blog/cybersecurity-statistics/](http://www.varonis.com/blog/cybersecurity-statistics/)
- 3Merriam-Webster. (2021). Cyberattack. From [www.merriam-webster.com/dictionary/cyberattack](http://www.merriam-webster.com/dictionary/cyberattack)
- 4Security.org. (1995-2021). How Secure Is My Password? From <http://howsecureismypassword.net> now being maintained at [www.security.org/how-secure-is-my-password/](http://www.security.org/how-secure-is-my-password/)
- 5Sobers, Rob. (2021). 134 Cybersecurity Statistics and Trends for 2021. From [www.varonis.com/blog/cybersecurity-statistics/](http://www.varonis.com/blog/cybersecurity-statistics/)





LIABILITY BEAT



# ELEVENTH CIRCUIT UPHOLDS IMMUNITY FOR OFFICER WHO SHOT MAN ARMED WITH A MASERATI

by Brian S. Batterton, J.D., LLRMI





*On April 2, 2020, the Eleventh Circuit Court of Appeals decided L.T. v. Owens et al.[i], which serves as an excellent review of the law related to deadly force.*

### **The Facts**

The facts of this case are lengthy; however, because use of force cases are very factspecific, it is beneficial to include all of the facts. The relevant facts of Owens, taken directly from the case, are as follows:

On the afternoon of March 24, 2015, three uniformed Smyrna police officers—Owens, Mark Cole, and Chris Graeff (collectively, the “Smyrna officers”)—and three uniformed Cobb County police officers—Daniel Mangold, Bryan Moore, and Robert Dorsey (collectively, the “Cobb officers”)—went to serve an arrest warrant on Thomas at a Goodyear store in Cobb County, Georgia, where Thomas worked. The parties agree that the following aerial image accurately depicts the Goodyear store and its environs on that date. Like the parties, we rely on the directions represented on the image, though we do not vouch for their accuracy.

Before arriving at Goodyear, the officers met in a nearby Publix parking lot to plan an approach. During this meeting, the officers reviewed a copy of the warrant, which was for technical probation violations, and discussed pertinent information about Thomas from a law enforcement database, including that he had “violent tendencies” and a prior history of “aggravated assault/fleeing or attempting to elude.”

After the briefing, the Smyrna officers drove to Goodyear in their respective marked patrol cars and parked in a

line, effectively blocking the only way to enter or leave the premises in a car without jumping a curb. They exited their cars and split up. Meanwhile, Mangold and Moore approached Goodyear on foot from the Publix parking lot and positioned themselves near the south end of the premises. Dorsey arrived at Goodyear soon after and parked beside the Smyrna officers’ cars, completely blocking the driveway.

The plan was for the Smyrna officers to attempt to execute the warrant at Goodyear while the Cobb officers remained outside in case Thomas attempted to flee on foot. Cole went to talk with some employees who were outside on the east of the building; Graeff approached the Goodyear lobby; and Owens remained near the patrol cars. The Goodyear employees told Cole that Thomas was driving a white Maserati—a customer’s car—that had just pulled around behind the building. Around this time, Owens heard what sounded like a “fastly accelerating vehicle” from behind the building.

What followed over the two minutes was a cat-and-mouse game contained within the Goodyear parking lot. Thomas made five passes behind the building on its west side in the Maserati, three going forward and two going backward. Throughout this time, the officers chased the car on foot and, each time the car stopped and changed directions, ordered Thomas at gunpoint to stop and exit the car. Thomas was shot and killed on the fifth pass.

Thomas made the first pass just as the officers were arriving. Beginning near the front (east) side of the

building, Thomas drove the Maserati clockwise around the building, ultimately ending up on the north end, his escape blocked by the line of police vehicles. Cole yelled out that Thomas was in the Maserati, and the Smyrna officers ran to meet it on the north end of the building. When they arrived, they ordered Thomas at gunpoint to stop and exit the car.

On the second pass, Thomas reversed, went around the northwest corner, and accelerated backward towards the southwest corner, where he stopped the Maserati about ten feet from the place Cobb officer Moore was stationed. Moore, at gunpoint, yelled for Thomas to stop and exit the car. Meanwhile, Cole ran to his truck and released his canine, Paco, believing that Thomas intended to flee on foot. Cole then joined Graeff in running after the Maserati.

The third pass was the opposite of the previous one. Just as Cole and Graeff rounded the northwest corner, they saw the Maserati quickly accelerate towards them down the middle of the paved pathway behind the building. Cole testified that Thomas tried to “run [him] over” and that he had “to jump out of the way” to avoid being hit by the oncoming car, which missed him by about a foot. Graeff testified that the car was coming towards them at “a high rate of speed” and that he “got as tight as [he] could” to the building to avoid the car as it passed. Video evidence corroborates their testimony. The video depicts two officers rounding the northwest corner in pursuit of the Maserati. Just after the officers appeared on the video, Thomas accelerated towards the officers and drove between them in very close proximity to one of the officers, who stepped aside when the car passed.

Thomas again drove around the northwest corner towards the parked patrol cars and came to a stop along the north end of the building.

On the fourth pass, Thomas reversed and headed back around the building in a counterclockwise direction, ultimately stopping near the southeast corner, where Cobb officer Mangold was located. Meanwhile, the Smyrna officers split up and ran after the Maserati. Video evidence depicts Owens running south on the back (west) side of Goodyear and going out of view near the southwest corner, where the north-facing camera was located. Cole, running in the same direction and holding his canine by the collar, went out of view about seven seconds later. Meanwhile, Graeff testified that he was on the east side of the building when he saw the Maserati accelerate forward after stopping at the southeast corner. He entered a bay door and cut through Goodyear’s interior service area, running to meet the car on the west side.

Thomas was shot and killed on the fifth and final pass. After sitting near the southeast corner for a few seconds, he accelerated the Maserati towards the southwest corner and began to turn. As the car was turning, Owens fired three shots in quick succession into the passenger side of the car, one of which struck Thomas causing his death. The Maserati continued forward, jumping the curb near the northwest corner and coming to rest on the grass. The officers broke the heavily tinted windows using less-lethal force and discovered that Thomas had been shot and was unresponsive. He was pronounced dead at the scene.

The central factual dispute concerns the location of Cole and Owens when Owens fired at Thomas. In Owens's version, he rounded the southwest corner and saw the Maserati, which was not moving, and ordered Thomas at gunpoint to stop and exit the car. The car then accelerated very quickly at him. Owens stepped back to avoid the oncoming car, which "just barely missed [him]," and then, seeing Cole approach the southwest corner in the path of the [1]turning car, fired three shots into the car's passenger side. Owens estimated that he began shooting when Cole was about ten feet in front of the car.

Cole's version of events differed from Owens's. When the shooting occurred, according to Cole, he was beside the Maserati, not in front of it, and "extremely close" to Owens. Just before the shooting, Cole explained, he had gained control of his dog, which was running loose until then, and began running down the backside of the building towards the southwest corner. He rounded the corner and saw the Maserati begin to accelerate, at which point his testimony becomes unclear. He indicated that, as the car accelerated forward, he "turn[ed] around with [his] dog" and started "going back in the opposite direction." When asked whether he was "in the path of the car" and whether it was "coming at you," Cole could not provide a clear answer. He responded that he was "very close to the car" and that it passed by him in "close proximity." He estimated that he was beside the front passenger window and "going back in that direction" when he heard the first of three gunshots from "right behind [him] on [his] left side." Cole stressed that he did not know why Owens fired his gun but assumed that Owens "saw something that I

couldn't see."

The record contains no other witness testimony about the shooting. Nevertheless, Plaintiffs propose a third version of events regarding the final pass. Plaintiffs contend that Cole and Owen both had reached the Maserati on the south end and were located on either side of the car when it began to accelerate. Then, according to Plaintiffs, the officers chased after the car, which posed no danger to them, and Owens fired three shots as the car rounded the southwest corner.

In support of this version of events, Plaintiffs cite Cole's interview with Cobb police investigators after the incident, during which Cole identified the south end of the building as where he struck the driver's side window of the stopped Maserati with his baton. That, in turn, would place Cole to the side of Thomas's car on the south end before the final pass. Arguably consistent with this version of events, Cole testified that, after running south around the southwest corner and seeing the Maserati accelerate, he "turned around" and started "going back in the opposite direction"—suggesting that Cole may have been running after the car when Owens opened fire.

*Construing the evidence in the light most favorable to Plaintiffs, we can rule out that Cole was in the path of the Maserati when Owens opened fire. Cole testified that he was beside the car when he heard the first gunshot and did not know why Owens shot. We also know that Owens was not in immediate personal danger when he fired at the Maserati, which had passed him. And there were no other*



*officers in the immediate path of the car at the time of the shooting.*

*As to whether Cole was beside or behind the car when Owens opened fire, we will assume without deciding that a reasonable jury could conclude that neither Owens nor Cole was in imminent danger of being hit near the southwest corner when Owens shot and killed Thomas.[ii] (emphasis added)*



Thomas's estate sued the officers involved in the shooting and the City of Smyrna for violating Thomas's right to be free from excessive force under the Fourth Amendment. The district court granted summary judgment and qualified immunity to all officers on the Fourth Amendment claim. Thomas's estate appealed the grant of summary judgment and qualified immunity. [Note: This article will not discuss the state law claims; however, it is noted that they were all dismissed by the district court.]

## **The General Legal Principles**

At the outset, it is important to understand that, when an officer is sued, he is entitled to qualified immunity from suit if he is acting in his discretionary authority. An officer is acting in his discretionary authority if the duty he is performing involves deciding between various options, such as what type of force to use when a suspect resists arrests. Thus, here, the officers were clearly acting within their discretionary authority. In order to defeat the officer's motion for qualified immunity, the plaintiff must satisfy a two-prong test. First, the plaintiff must show that the officer violated a federally protected right. Second, the plaintiff must show that the law was "clearly established" such that every reasonable officer in the same circumstance would have known that the conduct was unlawful.

Thus, the court set out to determine the first prong of the qualified immunity analysis, particularly whether the plaintiff has shown that the officers violated his rights under the Fourth Amendment by using excessive force. The court of appeals noted the legal principles that control this case. Particularly, the court stated

**The particular facts of each case must be analyzed to determine whether the force used was "objectively reasonable" under the totality of the circumstances.** *Graham v. Connor*, 490 U.S. 386, 396-97, 109 S. Ct. 1865, 104 L. Ed. 2d 443 (1989); see *Scott*, 550 U.S. at 382-83 (the reasonableness of a "use of a particular type of force in a particular situation" must be judged by the specific facts and circumstances confronting the officer). **To guide our analysis, we consider three main**

factors: “(1) the severity of the crime at issue; (2) whether [the suspect] posed an immediate threat to the officers or others; and (3) whether he actively resisted arrest.” *Penley v. Eslinger*, 605 F.3d 843, 850-51 (11th Cir. 2010); see *Graham*, 490 U.S. at 396. We also consider whether the officers issued a warning before using deadly force. *Penley*, 605 F.3d at 850. Nevertheless, there are no “rigid preconditions” for the use of force, and courts “must still slosh [their] way through the factbound morass of ‘reasonableness.’” *Scott*, 550 U.S. at 382-83.

We consider Owens’s conduct “from the perspective of a reasonable officer on the scene” and without regard to his “underlying intent or motivation.” *Kesinger v. Herrington*, 381 F.3d 1243, 1248 (11th Cir. 2004). In doing so, we must keep in mind that officers face situations that are often “tense, uncertain and rapidly evolving, thereby requiring split-second judgments as to how much force is necessary. Because an officer’s perspective in the field differs from that of a judge sitting peacefully in chambers, we must resist the temptation to judge an officer’s actions with the 20/20 vision of hindsight.” *Garczynski*, 573 F.3d at 1167 (quotation marks omitted).[iii]

### ***Shooting at Vehicles During Pursuits: When it’s Legal***

With these general principles in mind, the court then examined specific caselaw from the Eleventh Circuit related to the use of deadly force against people driving vehicles. The court first noted

**With regard to the use of deadly force against an individual who was driving a car, our cases “have...consistently upheld an officer’s use of force and granted qualified immunity in cases where the decedent used or threatened to use his car as a weapon to endanger officers or civilians immediately preceding the officer’s use of deadly force.”** *McCullough v. Antolini*, 559 F.3d 1201, 1207 (11th Cir. 2009).[iv]

The court then examined *Pace v. Capobianco*[v], in which the court upheld the use of deadly force against the driver a vehicle that had just led officers on a dangerous vehicle pursuit.

The court stated

We held that, even accepting that Davis did not try to run over the deputies or aim the car at the deputies, the use of force was justified because the officers had reason to believe that the car “had become a deadly weapon with which Davis was armed” and that the “chase was not over.” *Id.* at 1282. We noted that Davis had previously driven recklessly, threatening serious physical harm, that “Davis’s car was stopped for, at most, a very few seconds when shots were fired: no cooling time had passed for the officers in hot pursuit,” and that Davis had refused to get out of the car. *Id.* at 1281-82. [vi]

The court also examined *Long v. Slaton*[vii], which involved the use of deadly force against a suspect that resisted arrest, stolen a police car, and was trying to flee the scene. The court stated

We held that the officer’s decision to use deadly force was reasonable “in the light of the potential danger posed to officers and to the public if Long was allowed to flee in a stolen police cruiser.” *Id.* at 581. We noted that “the threat of danger to be assessed is not just the threat to officers at the moment, but also to the officers and other persons if the chase went on.” *Id.* (quotation marks omitted). And we reasoned that, although Long had not yet used the police cruiser as a deadly weapon when the shooting occurred, “Long’s unstable frame of mind, energetic evasion of the deputy’s physical control, Long’s criminal act of stealing a police cruiser, and Long’s starting to drive—even after being warned of deadly force—to a public road gave the deputy reason to believe that Long was dangerous.” *Id.* at 581-82.[viii]

Thus, precedent shows that, where a suspect uses a car as a weapon or threatens to use a car as a weapon, the Eleventh Circuit typically upholds the use of deadly force as reasonable, as described in the cases above.

### ***Shooting at Vehicles in Pursuits: When it’s Not Legal***

However, the court also discussed precedent where a suspect flees but does not use his vehicle as a weapon or threaten anyone with the vehicle. The court stated

**[W]here the plaintiff did not use or did not threaten to use his car as a weapon, we have rejected an officer’s use of deadly force.”** Morton v. Kirkwood, 707 F.3d 1276, 1283 (11th Cir. 2013).[ix]

The court then discussed *Vaughn v. Cox*[x], which involved the pursuit of a suspected stolen truck that fled to speeds of about 85 mph in a 70 mph zone. An officer put his police vehicle in front of the truck and applied his brakes. The truck crashed into the rear of the police car and continued to flee, driving 85 mph and staying within its lane. It did not swerve or drive toward other motorists. An officer drove next to the truck and fired three rounds into the **truck. The passenger was struck and was paralyzed. The court stated**

We concluded that a reasonable jury could find that the use of deadly force was unconstitutional because “[g]enuine issues of material fact remain[ed] as to whether [the truck’s] flight presented an immediate threat of serious harm... at the time [the officer] fired the shot.” *Id.* at 1330. We explained that, under the plaintiff’s version of the facts, “the truck’s lane was clear of traffic,” it did not make any “aggressive moves to change lanes,”



The Constitution allows some exceptions to the general prohibition against warrantless entry into a home, including where “exigent circumstances” exist. *Id.* Exigent circumstances may include “danger to the arresting officers...”

and the collision was “both accidental and insufficient to cause [the officer] to lose control.” Id. In short, the suspects were merely speeding by ten to fifteen miles per hour in an attempt to avoid capture. Id. Id. at 1331.<sup>[xi]</sup>

#### *Analysis of the Case At Hand – Was it legal to shoot Thomas?*



The court then set out to apply the general legal principles and caselaw to the facts of the case at hand. The court stated that the issue was [W]hether a reasonable officer in Owens’s position could have believed that Thomas posed an immediate threat of serious physical harm to police officers or others at the time of the shooting. In other words, would [Thomas] have appeared to reasonable police officers to have been gravely dangerous? <sup>[xii]</sup>

The court held, for the reasons discussed below, that even if we assume that the officers were to the side of Thomas’s vehicle and not in imminent danger of being hit at the time they fired their weapons, it was reasonable for the officers to believe that Thomas was

gravely dangerous, and as such, the shooting did not violate the Fourth Amendment.<sup>[xiii]</sup>

The reasons for the above holding are discussed below.

First, the officer had probable cause to believe that Thomas used the Maserati as a deadly weapon by threatening serious physical harm to officers on the scene. The evidence showed, including video evidence, that Thomas drove the Maserati around the building, stopped and then, as officers rounded the corner on foot, rapidly accelerated toward them so that they had to take evasive action to avoid being hit. The vehicle passed as close as one foot to one of the officers. This provided the officers with probable cause to believe that Thomas had committed aggravated assault in violation of Georgia law. The court further stated

**Although no deadly force was used at that time, it clearly would have been justified. *See Singletary v. Vargas*, 804 F.3d 1174, 1184 (11th Cir. 2015) (“[I]t is well established that an officer may constitutionally use deadly force when his life is threatened by a car that is being used as a deadly weapon.”); *Robinson v. Arrugueta*, 415 F.3d 1252, 1256 (11th Cir. 2005)** (upholding an officer’s use of deadly force against a suspect who slowly—at one or two miles per hour—drove a vehicle toward the officer as he stood between the suspect’s vehicle and a parked car). **Owens’s use of deadly force occurred less than one minute later, while Thomas was still dangerously speeding in the Maserati around the Goodyear facility. So this factor supports the reasonableness of Owens’s**



**actions.[xiv]**

Second, Thomas actively resisted arrest by fleeing in the Maserati, driving toward officers in an attempt to escape and refusing verbal commands at gunpoint given by officers. The court stated that this weighs in favor of the use of the force being reasonable.

Third, the court stated that the officers had probable cause to believe that Thomas posed an ongoing threat of serious physical harm to officers on the scene.

Specifically, the court stated

Plaintiffs stress that, under their version of facts, no officer was in the immediate path of the vehicle at the time of the shooting. But “the threat of danger to be assessed is not just the threat to officers at the moment, but also to the officers and other persons if the chase went on...”

And here, Thomas had shown no signs of giving up the chase or slowing down. He repeatedly ignored officer commands at gunpoint to stop and exit the car. And he evaded apprehension by accelerating back and forth in the Goodyear parking lot, taking tight corners at speeds—on the final pass, according to Plaintiffs’ expert, Thomas averaged 24.79 miles per hour on the backside of the building—that were high enough to pose a threat of serious bodily harm to persons on foot. Meanwhile, at least five officers were in active pursuit of the Maserati on foot, and other employees were on the premises. So, assuming Cole and Owens were outside of immediate danger at the time of the shooting, there were still at least

three officers running around on foot. For instance, Graeff testified that, on the fifth pass after the shooting, the Maserati passed in front of him just before he emerged from one of the bay doors on the west wide. **Because Thomas had not shown any signs of giving up the chase, the danger posed to the officers, and arguably others on the premises, still existed when Owens fired at Thomas.[xv]**

The court went on to explain that while no officer may have been in the direct path of the Maserati at the time of the shooting, the danger was still “sufficiently immediate” under caselaw to make deadly force reasonable, in light of the circumstances faced by the officers. The court stated

**While no officer was in the immediate path of the Maserati at the time of the shooting, the danger was sufficiently immediate under our caselaw to make the use of deadly force reasonable under the totality of the circumstances. Under these circumstances, the officers did not have to wait for Thomas to actually hit someone to take action. See Long, 508 F.3d at 581 (“[T]he law does not require officers in a tense and dangerous situation to wait until the moment a suspect uses a deadly weapon to act to stop the suspect.”); Pace, 283 F.3d at 1281-82. “Even if in hindsight the facts show that [the officers] perhaps could have escaped unharmed, an objectively reasonable law enforcement officer could well have perceived that the moving vehicle was being used as a deadly weapon, especially after the**

**driver had been repeatedly ordered to stop.”**

*Terrell v. Smith*, 668 F.3d 1244, 1255 (11th Cir. 2012) (citation and quotation marks omitted). **Based on the chaotic and quickly unfolding circumstances in the Goodyear parking lot, we cannot say it was unreasonable for Owens to use deadly force.[xvi]**

Therefore, plaintiff did not satisfy the first prong of the test to defeat the officer’s qualified immunity.

The court also noted that, for the sake of argument, if one were to assume the shooting was not reasonable under the Fourth Amendment, an examination of the second prong of the qualified immunity test reveals that the law is not clearly established such that a reasonable officer would have known deadly force was [hypothetically] unlawful under those circumstances. As such, the officers would still be entitled to qualified immunity.

Thus, the Eleventh Circuit affirmed the district court’s grant of qualified immunity for the officers in this case.

---

#### Citations

- [i] 2020 U.S. App. LEXIS 10387
- [ii] Id. at 2-10
- [iii] Id. at 14-15 (emphasis added)
- [iv] Id. at 15-16 (emphasis added)
- [v] 283 F.3d 1275, 1281-82 (11th Cir. 2002).
- [vi] Owens at 16
- [vii] 508 F.3d 576, 578-79 (11th Cir. 2007).
- [viii] Owens at 17
- [ix] Id.
- [x] ] 343 F.3d at 1330.
- [xi] Owens at 18-19
- [xii] Id. at 19
- [xiii] Id.
- [xiv] Id. at 21
- [xv] Id. at 22-24
- [xvi] Id. at 24 (emphasis added)



# Mitigating STRESS REACTION



by Natalie Sellers,  
LGRMS Law Enforcement Risk Consultant

In the famous words of Gordon Graham, “Do you have problems lying in wait with your...?” The success of any risk management plan hinges on the ability to not only recognize “seen” problems, but unforeseeable problems as well, within your agency.

Most of what law enforcement officers do, is done right. One could say that is due to proper training. Training is crucial, yet it can also be detrimental to a person’s decision-making process. The only way to know if your departmental training program is having adverse results, is to find out if you have problems lying in wait. Much of the job is repetition and therefore, good decision-making relies on good training.

The reason is because everyone is vulnerable to mistakes and slip-ups in routine repetitive tasks. For example, have you ever had to replace a debit card and when you got the new card, you were constantly putting in the old number? Or have you ever rented a car that was different from your own and reached down to shift into drive, only to find the gear shift was on the column?

When repetitive tasks are performed in stressful situations, decision-making is affected and can have a devastating effect on the outcome. Many occupations

face stressful, complex situations that require quick decision-making skills. And law enforcement is no exception.

Recognition-primed decision (RPD), as discussed by Gary A. Klein in *Sources of Power*, is a model of how people make quick, effective decisions when faced with complex situations. In Klein’s model, the decision maker is expected to identify the problem, compare it to previous similar situations and outcomes, and select the first course of action that will work to resolve the problem. The brain then falls back on what it has done, or been trained to do, in the past.

In law enforcement, we refer to this as “muscle memory”. This theory assists in understanding what happens in conditions of time pressure. Those extremely rare and risky events require good training for favorable outcomes. Good scenario-based training can help develop muscle memory that is pertinent to making decisions in rapidly evolving situations. The culture of an organization, onboarding, field training, and performance evaluations have an impact on an officer’s decision-making skills as well.

Kim Potter was certainly not the first officer to accident-



ly use her firearm instead of Taser. Research shows that this type of event has happened nine documented times since 2001. (EXPLAINER: How does an officer use a gun instead of a Taser? (apnews.com))

There have been many controls put in place to prevent this type of mistake from happening. Weak-side carry, color, weight, and feel of the Taser are all controls put in place to prevent mistakes. The one control that was left out was the operator in stressful situations. How do you manage human error?

The Yerkes-Dodson law is the theory that there is an optimal level of arousal that results in optimal performance. Too little arousal does not provide much in the way of motivation. Too much arousal causes a stronger stress reaction that can hamper performance. That optimal level of arousal differs from person to person, according to factors like the specific task, degree of skill, and confidence level. And getting to that optimal arousal zone can be difficult, because some factors are not within your control. But the Yerkes-Dodson law shows that there may be a sweet spot for achieving your best performance.

With that in mind, is your training program helping your officers familiarize themselves with the optimum level of arousal that results in their optimal performance level? Such training can help mitigate the frequency of error in the field. Subjecting officers to stressful situations in training will not only help to handle future situations, but it can also identify those who are unable to perform well under stress.

Navy Seal training is so rigorous and intense that it reprograms the candidates' brains by removing emotional response.

"We introduce our students, on day one, to absolute chaos. When you look at historic mistakes on the battlefield, they are almost always associated with fear and panic. So, the capacity to control these impulses is extremely important." Capt. Roger Herbert, then-commander of the SEAL training program at Coronado Island

One close-quarters combat exercise, the hooded box drill, involves putting a hood on a SEAL candidate that renders them blind and deaf, and then putting them in a

combat situation. The hood is finally ripped off and the candidate must respond in seconds.

"Sometimes, the response needs to be lethal and sometimes it needs to be nonviolent. Panic is not an option. Constant exposure to fear results in experiencing suppressed emotional responses and less lag time between the fear response and the frontal lobe logic process." (Navy SEAL brains are trained to alter how they process fear - We Are the Mighty)

Caliber Press provided a great example in their article, "It's a Matter of Time", of how quickly an officer must decide to use force. Video taken from the officer's body camera that involved a Chicago Police Officer and a 13-year-old boy revealed the officer had to make his decision to use force in 838 milliseconds. (Calibre Press |Developing Smarter, Safer, More Successful Law Enforcement Officers)

Does your departmental training program prepare your officers to use frontal lobe logic process or will it be a fear response? There is a time for classroom and online training. However, without exposure to scenario-based training, how will your officers suppress the emotional response? Learning optimal stress levels in scenario-based training will better prepare officers not to panic and to make good decisions.

A good training program helps develop and build self-confidence to make good decisions in rapidly evolving circumstances. It will also build departmental culture that is based on proper guidance from field training staff and policy.

From a liability perspective, training is also a critical component for avoiding liability lawsuits. Through several previous decisions, the courts have clearly established that law enforcement must conduct firearms training on a regular basis, it must reflect the environment they are likely to face (day and nighttime), and agencies must conduct decision-making training with respect to when to use deadly force. Furthermore, they have stated that annual and semi-annual qualification courses are simply insufficient for purposes of assisting officers in making deadly force decisions. (Critical Task for Patrol Officers; J. Ryan)

Training serves multiple purposes:



1. It is a process toward high-level performance by police.
2. Removes opportunity for deliberate indifference claims.
3. Is a means toward proper officer performance.

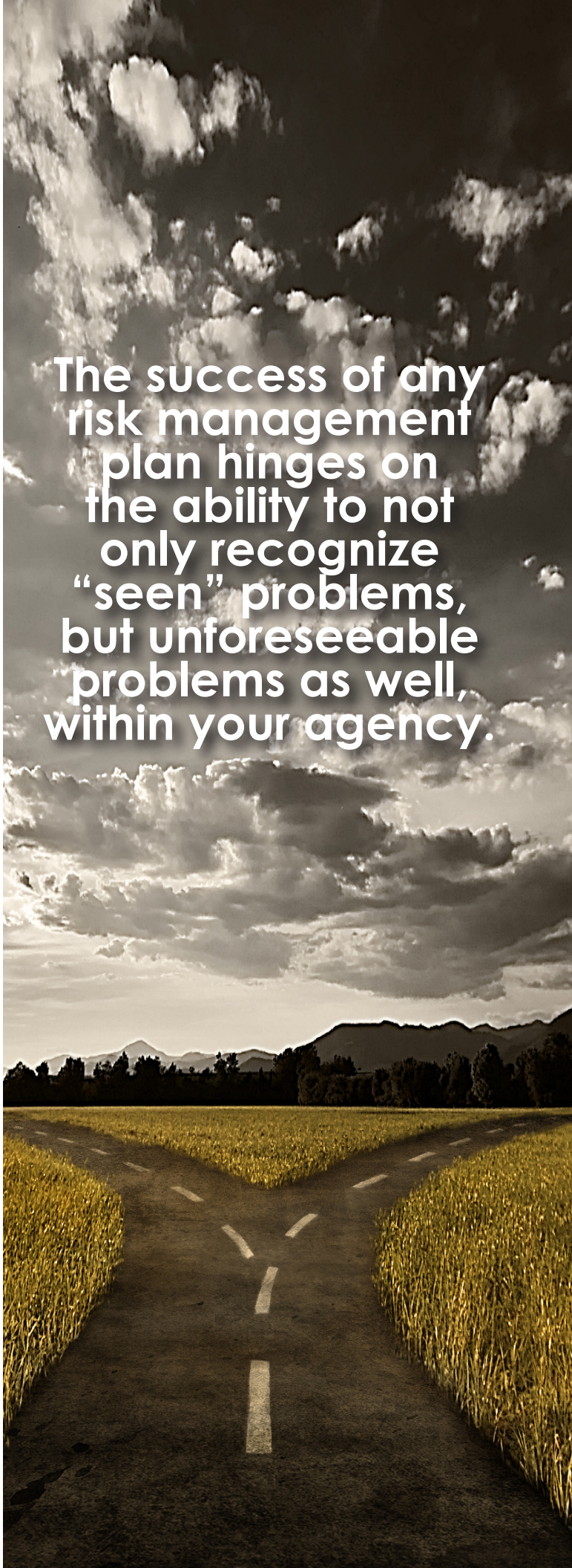
We hope you will take this opportunity to identify any problems lying in wait with regards to your training program. If we can assist with an audit of your training program or provide onsite scenario-based training, please contact your local field representative.

### References

Murphy, Sean. (2021). EXPLAINER: How does an officer use a gun instead of a taser? From <https://apnews.com/article/how-does-police-use-gun-instead-of-taser-explained-e6bb9c49b1bcd244e3ec11d94137c82>

Stilwell, Blake. (2021). Navy SEAL brains are trained to alter how they process fear. From <https://www.wearethemighty.com/mighty-trending/navy-seals-suppress-fear/>

Calibre Press. (2021). VIDEO: It's a Matter of Time. From <https://calibrepress.com/2021/04/video-its-a-matter-of-time/>

A dramatic landscape photograph showing a road that splits into two paths, leading into a vast field of golden crops. The sky is filled with large, textured clouds, and distant mountains are visible on the horizon. The overall tone is somber and contemplative.

The success of any risk management plan hinges on the ability to not only recognize “seen” problems, but unforeseeable problems as well, within your agency.



# NOTES FROM THE ROAD



## REOPENING THE STATE

by  
Steve Shields, LGRMS Loss Control Manager

The State is reopening. Did you ever think you would hear those words? I know I didn't, yet here we are. The State is slowly opening back up. For the Braves/United sports fans, it means they are going back to 100% capacity. It's a move back to normal life, but what does it mean to us?

Government employees remained on the front line from the beginning of the pandemic. Administration, recreation, and some other departments started working remotely, but the majority of employees had to be on the job to keep everything flowing as it should. Now that others are returning, I think we have to keep in mind how we interact with them. Some people literally haven't been outside of their home/driveway for almost a year, and they will possibly be very nervous and hesitant when around other people. I think we need to keep that in mind when dealing with the general public or other employees. I know that may be tough when you haven't missed a beat in your job, but that is the reality we face. As more and

more people return back to their offices, we will need to have patience and we can all get back to normal ASAP.

As I started this article, I thought about how life on the road has taken on new meaning for the staff of LGRMS. When visiting our members, we will need to keep in mind our contacts may be the person who is struggling with face to face meetings and adjust. We will get back to normal, it may be a new normal, but we will together get there.

Until next month, this is Steve Shields with Notes from the Road.





# American Policing:

## Strategies and Tactics



by David Trotter,  
LGRMS Senior Public Safety Risk Consultant



In the wake of many highly publicized Law Enforcement incidents nationwide, most currently the trial of former Minneapolis police officer Derek Chauvin, Law Enforcement operations have come under extreme scrutiny and criticism. Anyone who has attended Criminal Justice courses is familiar with Sir Robert Peel and the history of American policing. Just briefly, Sir Robert Peel is regarded as the father of modern British Policing. American Policing was created following British Policing principals and was basically a volunteer informal watch to warn the community of impending danger, primarily fires. Boston, New York, and Philadelphia created the first night watch systems in America. Formal Police Departments started to be created in the 1830's. These formal police departments were formed by city governments and employed full-time, paid police officers that were accountable to the public and the city. These early organizations followed

the principals of Sir Robert Peel and his 9 Policing Principals.

Those 9 principals hold true today in Law Enforcement policies and procedures. One of the most important is principal #7. "To maintain at all times a relationship with the public that gives reality to the historic tradition that the police are the public and that the public are the police, the police being only members of the public who are paid to give fulltime attention to duties, which are incumbent on every citizen in the interest of community welfare and existence."

Law Enforcement in the United States is a complex profession. We are given many duties and powers, which we must hold in the highest regard. Officers/deputies on a local government level are especially

part of the community and culture. Those duties and responsibilities come easier with the public's help and understanding. Connecting with members of the community, especially the informal leaders, gains respect and cooperation when things go sideways, and the officer/deputy must use force in an incident. Get out of the car and meet people. Talk to them. They will tell you what is needed in the community and will be willing to help accomplish that goal. Community policing is not new. It has been around since the inception of Law Enforcement. It is easy to lose sight of the advantages of community policing and easy to develop an "us vs. them" mentality. Community policing is not "hug-a-thug" it is getting to know the people in a community to be better able to serve them and get the job done. The goals are the same, you may just have to adjust the path to get there. That can make a difference in any incident to come to a more peaceful outcome.

“

...the police are  
the public and  
that the public  
are the police..







# Fun WITH SAFETY

Who said safety can't be fun? Test your knowledge and see how much you have retained from the articles in this month's SHARE Newsletter. The puzzles below and on the adjoining page can be solved using words and clues scattered throughout the publication.

**Check your answers to the crossword puzzle on p. 35.**

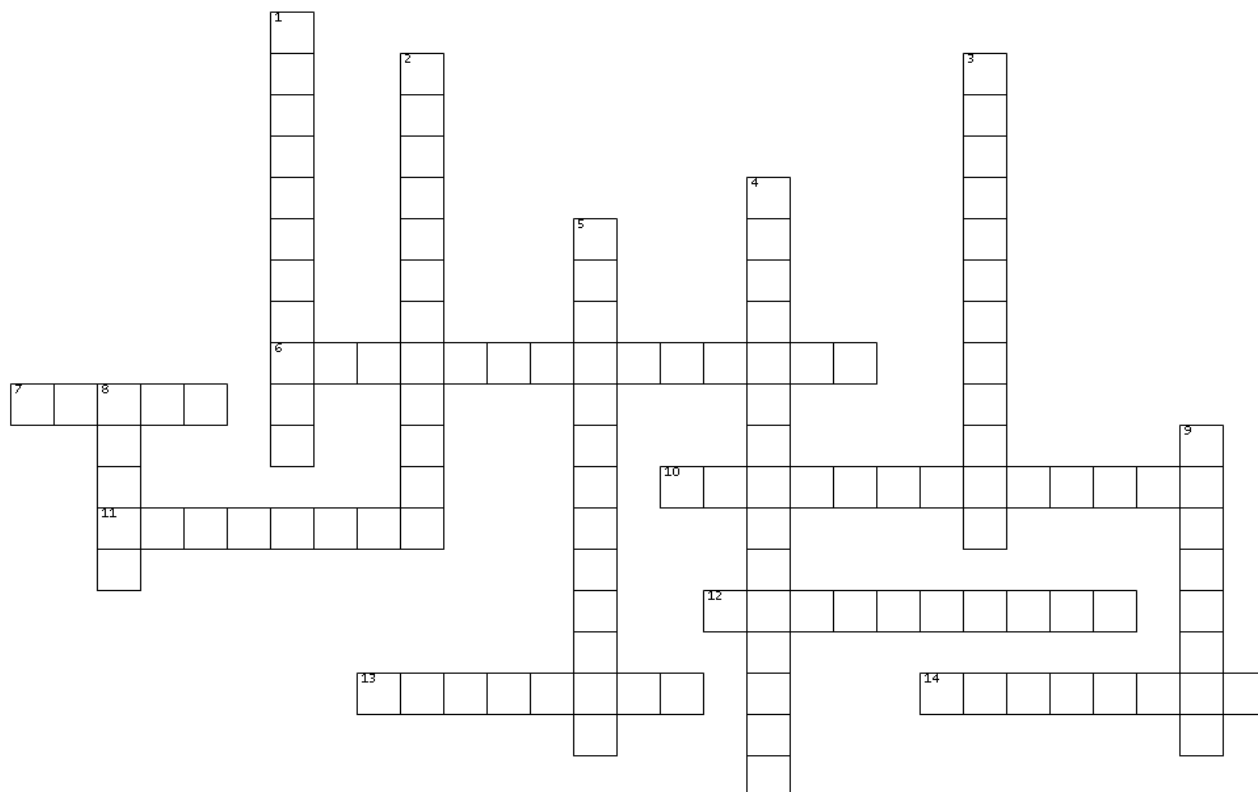
G	C	F	N	P	K	V	X	W	J	O	R	B	T	C
X	A	H	C	S	P	X	V	A	T	Z	V	G	I	R
C	Y	B	E	R	A	T	T	A	C	K	E	N	U	I
X	J	L	N	M	I	I	G	F	O	O	L	I	C	M
Y	W	E	A	U	I	N	Y	U	T	D	Y	T	R	I
O	Y	I	S	M	I	C	T	X	L	P	M	A	I	N
S	A	R	X	N	R	D	A	I	F	R	E	G	C	A
U	U	A	I	H	O	O	G	L	P	U	D	I	H	L
P	J	A	Z	O	O	Z	N	I	C	K	I	T	T	J
V	R	B	R	R	W	L	E	W	F	U	S	I	N	U
T	O	S	A	R	J	A	S	C	E	D	E	M	E	S
S	E	S	S	A	L	G	N	U	S	N	A	S	V	T
G	N	I	N	E	P	O	E	R	D	H	S	N	E	I
L	M	Z	D	I	C	J	H	X	H	D	E	V	L	C
W	R	I	Y	Z	K	X	O	V	Q	A	F	L	E	E

- |                       |                        |
|-----------------------|------------------------|
| 1. Cyber Attack       | 9. Criminal Justice    |
| 2. Social Engineering | 10. Community Policing |
| 3. Chemical Cues      | 11. Reopening          |
| 4. Lyme Disease       | 12. New Normal         |
| 5. Outdoors           | 13. Mitigating         |
| 6. Sunglasses         | 14. Training           |
| 7. Eleventh Circuit   |                        |
| 8. Pursuit            |                        |

# MAY SHARE Crossword PUZZLE



## SHARE Crossword Puzzle - May



### ACROSS

6. a complex profession in the United States
7. type of bugs that spend the majority of their time waiting to attach themselves to a host
10. sufficient reason based upon known facts to believe a crime has been committed
11. when an officer is sued he is entitled to qualified what if acting in discretionary authority
12. these employees remained on the front line from the beginning of the pandemic
13. use fine tipped versions of these when removing ticks
14. generic and widespread emails that lure you into clicking a link or opening attachments

### DOWN

1. type of sun rays that can damage your skin in as little as 15minutes
2. when the brain falls back on what it has been trained to do in the past
3. these exposed 36 billion records in the first half of 2020
4. theory that there is an optimal level of arousal that results in optimal performance
5. the father or modern British policing
8. 9, consider how this is spreading in your community when choosing safer activities
9. some will be very nervous and this when venturing out after the pandemic





LIVING WELL GEORGIA

## SAFETY TIPS

FOR BEING IN THE SUN,  
GOING BACK OUT AGAIN  
AND A FORUM CALL



by Candace Amos,  
LGRMS Health Promotion Representative



Spring is officially here and the sun is shining! That means lots of high temperatures as well as celebrations, festivities, and gatherings. So, what are some best forms of protection while enjoying time outside? Keep reading below for sun and outdoor safety tips.

### **Seek Shade**

The sun's ultraviolet (UV) rays can damage your skin in as little as 15 minutes. You can reduce your risk of skin damage and skin cancer by seeking shade under an umbrella, tree, or other shelter before you need relief from the sun.

### **Dress in Protective Clothing**

When possible, long-sleeved shirts and long pants and skirts can provide protection from UV rays. Clothes made from tightly woven fabric offer the best protection. If wearing this type of clothing isn't practical, at least try to wear a T-shirt or a beach cover-up.

### **Wear a Hat**

For the most protection, wear a hat with a brim all the way around that shades your face, ears, and the back of your neck. A tightly woven fabric, such as canvas, works best to protect your skin from UV rays. Avoid straw hats with holes that let sunlight through. A darker hat may offer more UV protection. If you wear a baseball cap, you should also protect your ears and the back of your neck by wearing clothing that covers those areas.

### **Have on Sunglasses**

Sunglasses protect your eyes from UV rays and reduce the risk of cataracts. They also protect the tender skin

around your eyes from sun exposure. Sunglasses that block both UVA and UVB rays offer the best protection. Wrap-around sunglasses work best because they block UV rays from sneaking in from the side.

### **Put on Sunscreen**

Put on broad-spectrum sunscreen with SPF 15 or higher before you go outside, even on slightly cloudy or cool days. Don't forget to put a thick layer on all parts of exposed skin. Get help for hard-to-reach places like your back. And remember, sunscreen works best when combined with other options to prevent UV damage.

### **Know the Warning Signs of Heat Exhaustion and Heat Stroke**

Recognize the warning signs of both. Heat exhaustion is when you might feel dizzy, lightheaded, or like you are going to faint. Headache is also a symptom. Lie down in a shady area, drink water, and rest. Heat stroke is much more serious. People can die from heat stroke. The body's temperature soars and the pulse races. Cool down by removing clothes and immersing in cold water, if possible. Get medical help immediately.

### **Choose Safer Activities**

When choosing safer activities, consider how COVID-19 is spreading in your community, the number of people participating in the activity, and the location of the activity. Outdoor visits/activities are safer than indoor visits/activities, and many are starting to go back out again to do things they had stopped doing, because of the pandemic. For more information, please visit: [Choosing Safer Activities | CDC](#).



By following these sun and outdoor safety tips, you're not only protecting yourself, but representing that wellbeing and health is important to you. And there are many ways you can improve your health, as well as your employees' health. You can start by participating in the LGRMS HPS Forum Call, in which we'll go over a Health Toolkit that provides "tools" to promote health in your organization.

**The Health Toolkit** will be placed in the next issue of the SHARE newsletter, following the Forum Call, but it will be for the upcoming month. You'll receive all the tools you'll need beforehand to start planning.

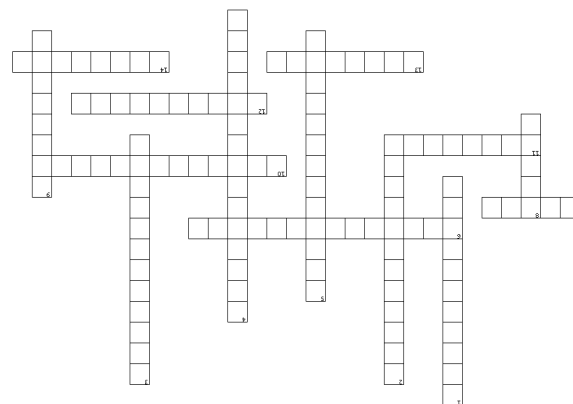
**The Forum Call** is for Health Promotion Champions and individuals responsible as health promotion leaders, administrators, HR and personnel directors, clerks, health/safety coordinators, and wellness/health benefit coordinators. All are welcome to participate. You'll receive an invite each month. Please stay on the lookout!

#### Sources

Centers for Disease Control and Prevention (CDC). 2020. Sun Safety. From [https://www.cdc.gov/cancer/skin/basic\\_info/outdoors.htm](https://www.cdc.gov/cancer/skin/basic_info/outdoors.htm)

Centers for Disease Control and Prevention (CDC). 2021. Choosing Safer Activities. From <https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/participate-in-activities.html>

Family Safety & Health, Vol. 62, No. 2 © HHI



**Across:** 6. Law Enforcement 7. Ticks 10. Probable cause 11. Immunity  
**Down:** 1. Ultraviolet 2. Muscle 12. Government 13. Tweezers 14. Fishing  
 3. Data breaches 4. Yerkes Dodson Law 5. Sir Robert Peel 8. COVID  
 9. Hesitant

Crossword Puzzle Answer Key





## Tick, Tick TICKED

It's time to be on the lookout  
for these unwanted hitchhikers!

## Tick, Tick, Tick . . .

No, this isn't an alarm clock!

Spring is here and summer is on the way. Now is the time to be aware of those little critters called "ticks".

Ticks spend the majority of their time waiting to attach themselves to a host. Since they cannot run, hop, fly, or move quickly, they wait for the host to come near where they are—in shady areas, on tall grass, in brush or weeds, on fences, the sides of buildings—and then fall or snag a ride. They actually can detect nearby vibrations, use chemical cues, or detect shadows to find a potential host.

Once on the host, they insert their head into the skin and feed on the host's blood until they are full. Then, they drop off and go through their reproducing stage. Homes, workplaces, and vegetation can become infested through this process.

Ticks are very small and hard to detect; they can look like a mole, dirt, or a small dark spot on the skin or in your hair. Not all ticks carry diseases, but every precaution should be taken. Lyme Disease, Rocky Mountain Spotted Fever, and Southern tick associated rash illness are some of the illnesses associated with ticks. If a tick is found, remove it as soon as possible and watch for any type of rash, fever, feeling of weakness, headaches, joint pain, or other illness within the next thirty days. If any type of symptom appears, you need to immediately visit a health care provider.

## Precautions to Take

- Wear light-colored clothing so you can see them
- Tuck your pant legs into your socks, so they cannot crawl up onto your leg (some are small enough to go through socks).
- Use a repellent with DEET (skin & clothing) or with permethrin (for clothing) and read manufacturers' directions and warnings for how to use it and who it can be used on.
- After spending time in potentially tick infested areas, do a complete body check, paying attention to the waist, areas with body hair, back of knees, under the arms, around the ears, between the legs, and inside the belly button.
- Remove ticks immediately, using the proper procedure.
- Clothing should also be checked and ticks removed.

Visit the websites at the end of this article for additional information and pictures of the common ticks found in Georgia.

## Removal of ticks

The Georgia Department of Health does not recommend common home remedies such as lighting the tick on fire or covering it in petroleum jelly, nail polish, alcohol, or kerosene.

1. Grasp the tick as close to the skin surface as possible with fine-tipped tweezers.
2. Pull the tick straight out slowly. DO NOT squeeze or twist the tick while pulling it out.
3. Wash and treat the bite area with a disinfectant. You can save the tick in rubbing alcohol for identification.



## Additional Resources

<https://www.cdc.gov/ncezid/dvbd/media/stopticks.html>

<http://dph.georgia.gov/document/publication/all-about-ticks-common-human-biting-ticks-georgia/download>

<https://dph.georgia.gov>

[search?search=VBB+Brochure+2008&sm\\_site\\_](#)

[name=dph](#)





# General Self Inspection Program

[Click Here to Print Form](#)

Location, Area, or Department: \_\_\_\_\_ Date: \_\_\_\_\_

Surveyor: \_\_\_\_\_

## General Evaluation

	Needs Action	Needs Improvement	Good	Very Good
A. Property/Liability				
a. Fire protection	_____	_____	_____	_____
b. Housekeeping	_____	_____	_____	_____
c. Slip/trip/fall	_____	_____	_____	_____
d. Public safety	_____	_____	_____	_____
B. Employee Safety				
a. Safety meetings	_____	_____	_____	_____
b. Safety rules	_____	_____	_____	_____
c. Work conditions	_____	_____	_____	_____
d. Auto/equipment	_____	_____	_____	_____

## Property/Liability

	Yes	No
Fire protection	<input type="checkbox"/>	<input type="checkbox"/>
Emergency numbers posted	<input type="checkbox"/>	<input type="checkbox"/>
Fire extinguishers available/serviced	<input type="checkbox"/>	<input type="checkbox"/>
Fire alarm panel showing system is operational; no warning lights.	<input type="checkbox"/>	<input type="checkbox"/>
Automatic sprinkler system control valve locked in open position.	<input type="checkbox"/>	<input type="checkbox"/>
Automatic sprinkler heads clear of storage within three feet.	<input type="checkbox"/>	<input type="checkbox"/>
Flammable, combustible liquids stored in UL-listed containers.	<input type="checkbox"/>	<input type="checkbox"/>
Flammable, combustible liquid containers stored in proper cabinet or container.	<input type="checkbox"/>	<input type="checkbox"/>
Smoking, No Smoking areas designated/marked.	<input type="checkbox"/>	<input type="checkbox"/>
Any cigarette butts noticed in No Smoking areas.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_  
\_\_\_\_\_

## Housekeeping

Stairwells clear of combustible items.	<input type="checkbox"/>	<input type="checkbox"/>
Furnace, hot water heater, and electrical panel areas clear of combustible items.	<input type="checkbox"/>	<input type="checkbox"/>
Work and public areas are clear of extension cords, boxes, equipment, or other tripping hazards.	<input type="checkbox"/>	<input type="checkbox"/>
Floor surfaces kept clear of oils, other fluids, or water.	<input type="checkbox"/>	<input type="checkbox"/>
Stored items are not leaning or improperly supported; heavy items are not up high.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_  
\_\_\_\_\_

## Slip/Trip/Fall

Stair treads are in good condition; not worn, damaged or loose.	<input type="checkbox"/>	<input type="checkbox"/>
Handrails for all stairs/steps.	<input type="checkbox"/>	<input type="checkbox"/>
Guardrails for all elevated platforms.	<input type="checkbox"/>	<input type="checkbox"/>
Stair handrails are in good condition; not loose or broken.	<input type="checkbox"/>	<input type="checkbox"/>
Floor surfaces are even, with non-slip wax if applicable.	<input type="checkbox"/>	<input type="checkbox"/>
All rugs are held down or have non-slip backing.	<input type="checkbox"/>	<input type="checkbox"/>
Any holes, pits or depressions are marked with tape, barricades, or guardrails.	<input type="checkbox"/>	<input type="checkbox"/>
Wet floor signs are available and used.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_  
\_\_\_\_\_

## *General Self Inspection Program*

### ***Public Safety***

Yes                      No

Public areas kept clear of storage and supplies.	<input type="checkbox"/>	<input type="checkbox"/>
Emergency lighting for public assembly areas in buildings.	<input type="checkbox"/>	<input type="checkbox"/>
Evacuation plans posted for public assembly areas in buildings.	<input type="checkbox"/>	<input type="checkbox"/>
Public areas have necessary warning or directional signs.	<input type="checkbox"/>	<input type="checkbox"/>
Construction work has barriers, covers, and markings.	<input type="checkbox"/>	<input type="checkbox"/>
Street and road signs noted in good condition, clear of obstructions.	<input type="checkbox"/>	<input type="checkbox"/>
Sidewalks smooth and even; no holes, no raised or broken areas.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_

### ***Employee Safety***

#### **Safety Meetings**

Held in the department.	<input type="checkbox"/>	<input type="checkbox"/>
Meetings held    ___ monthly    ___ quarterly    ___ other _____ ; documented	<input type="checkbox"/>	<input type="checkbox"/>
Different topic each time.	<input type="checkbox"/>	<input type="checkbox"/>
Covers department safety rules.	<input type="checkbox"/>	<input type="checkbox"/>

#### **Safety Rules**

Rules specific for this department.	<input type="checkbox"/>	<input type="checkbox"/>
Rules are written, posted in the department.	<input type="checkbox"/>	<input type="checkbox"/>
Reviewed with new employees.	<input type="checkbox"/>	<input type="checkbox"/>

#### **Work Conditions**

Employees exposed to:    \_\_\_ Heat    \_\_\_ Cold    \_\_\_ Rain/sleet/snow    \_\_\_ Use of chemicals  
                                      \_\_\_ Noise    \_\_\_ Work in confined spaces    \_\_\_ Work in trenches  
                                      \_\_\_ Traffic    \_\_\_ Blood/body fluids    \_\_\_ Other \_\_\_\_\_

Proper personal protective equipment available

Respirators, goggles, face shields, chemical gloves, traffic vests, appropriate clothing  
 Trench boxes/shoring for trenching, ear plugs/muffs, body armor (law enforcement)  
 Confined space equipment, harness, air testing equipment, ventilation equipment, tripod  
 Fire department turn-out gear, blood-borne pathogens kits

Personal protective equipment required to be worn.	<input type="checkbox"/>	<input type="checkbox"/>
Employees trained on proper use.	<input type="checkbox"/>	<input type="checkbox"/>
Equipment properly maintained.	<input type="checkbox"/>	<input type="checkbox"/>
Shop equipment has proper guards to protect from pinch or caught-between type injuries.	<input type="checkbox"/>	<input type="checkbox"/>
Chemicals used in the department.	<input type="checkbox"/>	<input type="checkbox"/>
MSDS sheets available; employees trained on hazards, proper use, proper PPE to use.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_

### ***Auto and Equipment***

Seat belts provided.	<input type="checkbox"/>	<input type="checkbox"/>
Seat belts required to be used.	<input type="checkbox"/>	<input type="checkbox"/>
Drivers noted wearing seat belts.	<input type="checkbox"/>	<input type="checkbox"/>
All lights working including strobe lights, turn signals.	<input type="checkbox"/>	<input type="checkbox"/>
Tires in good condition, tread, sidewalls.	<input type="checkbox"/>	<input type="checkbox"/>
Glass in good condition; not cracked, broken.	<input type="checkbox"/>	<input type="checkbox"/>
Reflective tape, signs in good condition.	<input type="checkbox"/>	<input type="checkbox"/>
Any periodic, documented, self-inspection of the vehicles/equipment.	<input type="checkbox"/>	<input type="checkbox"/>
Proper guards on mowers, other equipment.	<input type="checkbox"/>	<input type="checkbox"/>

Comments: \_\_\_\_\_

# Safety Meeting Attendance Sign Up Sheet

[Click Here to Print Form](#)

City/County: \_\_\_\_\_

Date: \_\_\_\_\_

Department: \_\_\_\_\_

Topic: \_\_\_\_\_

Attendees:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Next meeting scheduled for \_\_\_\_\_

Safety Coordinator \_\_\_\_\_



# LGRMS CONTACTS 2021

## LGRMS HOME OFFICE

### Dan Beck

LGRMS Director  
[dbeck@lgrms.com](mailto:dbeck@lgrms.com)  
O: 678-686-6280  
C: 404.558-1874

### Tamara Chapman

Office Manager  
[tchapman@lgrms.com](mailto:tchapman@lgrms.com)  
O: 678-686-6283  
C: 404.623-8055

### Cortney Stepter

Administrative Coordinator  
[cstepter@lgrms.com](mailto:cstepter@lgrms.com)  
O: 678-686-6282

## PUBLIC SAFETY RISK CONTROL

### Dennis Watts

Training, Communication, and Public Safety  
Risk Manager  
[dwatts@lgrms.com](mailto:dwatts@lgrms.com)  
404.821.3974

### Mike Earl

Public Safety Risk Consultant  
[mearl@lgrms.com](mailto:mearl@lgrms.com)  
404.558.8525

### David Trotter

Senior Public Safety Risk Consultant  
[dtrotter@lgrms.com](mailto:dtrotter@lgrms.com)  
404.295.4979

### Natalie Sellers

Law Enforcement Risk Consultant  
[nsellers@lgrms.com](mailto:nsellers@lgrms.com)  
404.904.0074

## RISK CONTROL

### Steve Shields

Loss Control Manager  
[sshields@lgrms.com](mailto:sshields@lgrms.com)  
404.416.3920

### Chris Ryan

Loss Control Representative SW Region  
[cryan@lgrms.com](mailto:cryan@lgrms.com)  
229.942.2241

### Vincent Scott

Loss Control Representative SE Region  
[vscoff@lgrms.com](mailto:vscoff@lgrms.com)  
404.698.9614

## HEALTH PROMOTION SERVICES

### Sherea Robinson

Health Promotion Services Manager  
[srobinson@lgrms.com](mailto:srobinson@lgrms.com)  
404.821.4741

### Candace Amos

Health Promotion Representative  
SW Central Region  
[camos@lgrms.com](mailto:camos@lgrms.com)  
404.416.3379

## HEALTH PROMOTION SERVICES

(continued)

### Paige Rinehart

Health Promotion Representative  
NE Central Region  
[prinehart@lgrms.com](mailto:prinehart@lgrms.com)  
404.295.4979

## JOB POSTING

Do you possess a high level of customer service, team membership, communication and influence skills? Would you like to see your name listed among our team members? If so, this may be the position for you.

LGRMS IS SEARCHING FOR A

**SOUTH GEORGIA  
RISK CONSULTANT**

If Interested, please send your cover letter and resume to:  
[applications@gmanet.com](mailto:applications@gmanet.com)



# SHARE

**MAY 2021**  
**ISSUE #5**

## ANNOUNCEMENTS

### INTERESTED IN APPLYING

Send your cover letter and resume to: [applications@gmanet.com](mailto:applications@gmanet.com)

# HELP WANTED!

LGRMS IS SEARCHING FOR A

**SOUTH GEORGIA  
RISK CONSULTANT**

**SEE DESCRIPTION BELOW**

### MINIMUM QUALIFICATIONS

Bachelor's degree in related field required; some experience in program administration or a related field; or an equivalent combination of education, training, and experience which provides the requisite knowledge, skills, and abilities for this job. Must possess and maintain a valid Georgia driver's license.

- Career development strongly encouraged, with a potential for growth/advancement within LGRMS, GMA and ACCG
- Competitive salary and strong benefits package

### Go to:

[www.lgrms.com/resources](http://www.lgrms.com/resources)  
for more information.

### Location:

This position will be responsible for supporting approximately 200 members within Southern Georgia Region. The Southern Georgia Region has not been formally defined, but it is roughly the line from Quitman County/Georgetown to Effingham County/Springfield. It is preferable the person that holds the position live within or near the Southern Georgia Region.

### Salary/Benefits:

- Strong family and team working environment
- Ability to positively impact member employees' and citizens lives
- Based on the candidate's experience, we offer a six-month to two-year onboarding process to ensure their success in this new role

### The Ideal Candidate's Background/Experience:

- Although the Loss Control Consultant position reports to the Loss Control Manager, there is a great deal of independence and autonomy. Candidates should have a proven record of self-management and motivation.
- The position requires a high level of customer service, team membership, communication (written/verbal), and influence skills. Candidates should have a proven record of presenting, influencing or leading people from all levels of an organization.
- This position requires a high level of analytical and problem-solving skills. Candidates should have a proven record of conducting surveys or evaluations, loss & root-cause analysis, and making sound recommendations for long-term sustainable corrective actions.

# SHARE

**MAY 2021 - ISSUE 5.0**

LOCAL GOVERNMENT RISK  
MANAGEMENT SERVICES,  
INC., - A Service Organization  
of the ASSOCIATION COUNTY  
COMMISSIONERS OF GEORGIA  
and the GEORGIA MUNICIPAL  
ASSOCIATION

# VISIT THE LGRMS WEBSITE

For more information.

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

Has your organization undergone any changes in personnel? Are there other staff members that you would like to receive a copy of our publications? If so, please click the link below to download our contact list form.

[Contact List Form](#)



Local Government  
Risk Management Services  
3500 Parkway Lane . Suite 110  
Peachtree Corners, Georgia 30092