RMI INTERNATIONAL

RMI Insight

PROFESSIONAL SECURITY SERVICES

WINTER 2025 / RMI INTERNATIONAL INC.

A Message from HR

To all RMI personnel: RMI wishes to express our gratitude for all the hard work you have been doing on behalf of our company and our clients. Your dedication and diligence on the job help bolster the image of our company and profession in the eyes of our clients and their personnel, patrons, vendors and all others who arrive to do business at their locations.

Additionally, your continual efforts at striving to be the professionals you are, are instrumental in not only helping our clients to run their businesses safely and securely, but in also helping to assure return business as we will see below.

May we all continue to work together as a team in promoting excellence in 2025!

Sincerely,

Richard Aparicio
RMI Senior HR Manager

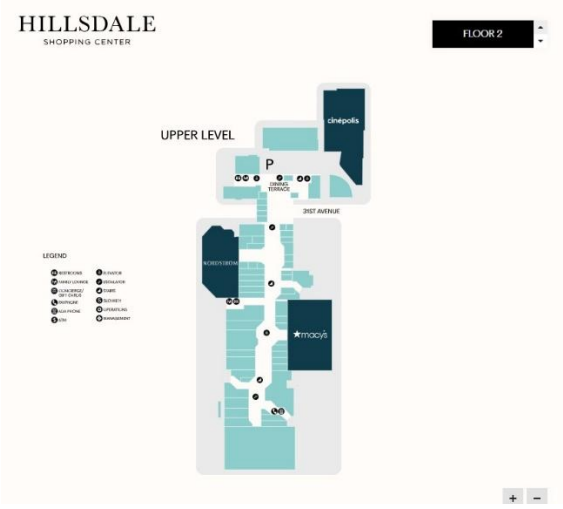
Returning Business

RMI is pleased to announce the following contract renewals with several of our existing clients:

Hillsdale Shopping Center; San Mateo, CA

The Center has 131 stores and is covered by RMI security and customer service personnel who:

- Patrol the parking lots and interior areas.
- Assist customers with information and directions.
- Respond to medical and other types of emergency situations and/or general service requests.



See Returning Business, p2.

Continued from p1.

Returning Business

Promenade at Downey, CA

The Promenade has 62 stores and is covered by RMI security personnel who:

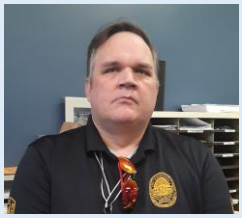
- Patrol the parking lots.
- Assist customers with information and directions.
- Respond to medical and other types of emergency situations.

Commerce Casino; City of Commerce, CA

The facility offers lodging, dining, event space and gambling and is covered by RMI security personnel who:

- Post on Towers in parking lots watching over general parking and access control for the employee parking lot.
- Assist customers with information and directions.
- Respond to medical and other types of emergency situations.

New Facility Supervision



William Johnston: RMI welcomes William Johnston as the new RMI-Honda Irving, TX facility security supervisor. William was born in Sherman, TX and lived in Mexico with his father when he worked for the State Department, until William was 8 years old. William then moved to Richardson, TX with his Grandparents.

William went to Richardson High School and played football for the Golden Eagles for 3 years. From there, he went to college for one year and then went to work for UPS where they sent him to their management school to learn the UPS policies and procedures to work in their loss prevention department as a supervisor for 6 years. He also worked for Texas Instruments for several years in a supervisor and in an investigator capacity where he worked an embezzlement case.

Mr. Johnston has worked in the security industry for several years, always in a supervisor or a manager capacity, and as of February of 2025 he is the new site security supervisor at the RMI-Honda facility at Irving, TX. William looks forward to being an integral part of RMI to make the site he has been assigned to a smooth-running operation.

Safety Corner

Spring Duty Precautions

With spring comes the arrival of various weather conditions, which RMI personnel need to be mindful of, whether they are performing their duties on foot or in a vehicle.

Things to consider:

- Wet Surfaces: With spring comes rain and if it has not rained for a while, surfaces may become very slick when rain mixes with oil and other fluids that have accumulated on the ground.

  Avoid walking and/or driving in slick areas and advise coworkers of trouble spots, if they are not already aware.

- Icy Surfaces: It can still be quite cold at some RMI locations in the Midwest and south and icy surfaces can be difficult to see.

  Take note of the temperature after a shower, especially at night or in shaded places, and check for ice before starting foot or vehicle duties.

  Exercise care around icy spots and also advise coworkers if they are not already aware.

- Fog: Springtime fog can also be an issue at some RMI post locations.

  Fog can make it difficult to see potentially dangerous situations around you to act or react in a timely manner to avoid them.

  Fog can also make surfaces slick, where RMI personnel walk and/or drive.

  Therefore, it is important to watch where you are walking and/or slow a vehicle down to a safe speed.

Note: RMI personnel should consult with their supervisor to temporarily suspend foot and/or vehicle duties where weather conditions require this.

Sincerely,

Richard Aparicio
RMI Senior HR Manager

Top Cyber Threats, 2025: (LMG Security Webinar 2/19/25)

Hackers are relentless in their efforts to access the personal or business data of others for various nefarious reasons. They are constantly working to perfect phishing scams, create malware, etc., to extort, embarrass, or otherwise harm their targets.

The following will provide a few examples of recent efforts on their part and suggested precautions.

- Hackers, using Worm GPT, sent a large number of phishing emails to business contacts to get unsuspecting personnel to reach out to their IT dept.

  They pretended to be a representative of the company's IT department, and they contacted their targets before employees reached out to their IT rep., already knowing that the employees had received the hackers' emails. They did this to get employees to utilize Teams or some other remote access software program to gain access to company computers for planting malware on them.

  They gained compliance by pressing employees with the urgency of the matter and obtained their cooperation in logging the hackers in.

  How can you help protect yourself against this type of attack? Know who your IT personnel are or how to verify them before providing cooperation. If you are not sure of who you are interacting with, reach out to a trusted source at a trusted number, or other method, before complying with them. Follow company IT policy.

- Hackers are also cloning legitimate business websites to lure employees and visitors to access them for the hacker to in turn gain computer/device access to unsuspecting people by them accessing a link, downloading a file, etc., from the fake website.

  Additionally, hackers are also cloning software and service provider accounts like DocuSign, PayPal, and other services a bank, a tax preparer, or a company might use for persons to sign docs, conduct other business, etc.

  In both instances above, if something looks off about the website you are visiting - especially if you have visited it before, or if you are asked to do something that does not seem correct for your business at hand, then you may want to make attempts to verify before proceeding.

  You can check the website's address, contact the company at a trusted number, etc., to discuss your concerns before proceeding.

  Note: The only operational apps RMI uses are Track Tik and ADP. RMI will never require any employee to enter personal or financial information for any work-related tasks. If employees are requested to provide personal or financial information they should stop and contact their manager.

- Hackers are finding ways past multi-factor authentication so it's suggested to use advanced protection where available – passkey (digital credential), biometrics (fingerprint, facial recognition, etc.), hardware tokens (USB, etc., password generator).

- AI scams are rapidly becoming more sophisticated. One video of yourself on social media is all it takes now to clone you – 1 minute of your speech can be used to create an effective voice tone/replica and a couple minutes of you on video can be used to create a video of you to fool your loved ones – especially the elderly.

  You may want to advise your contacts to reach out to you first, via trusted means, before sending money or following through on some other request that you supposedly are asking them to do and be careful to not fall prey yourself.

- It's recommended to purge or consolidate your sensitive data that is not needed. Or, if not needed to be readily accessible, maybe keep it somewhere secure that's not accessible via internet. Less personal data online, can be less to worry about.

- Know where personal products you are using are hosted – e.g., China, Russia, etc., and exercise caution when selecting for use.