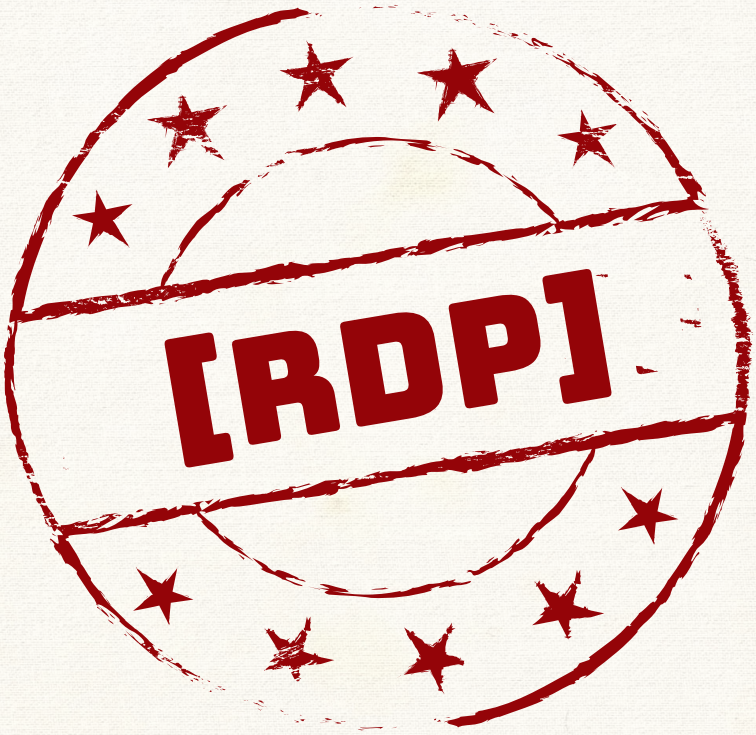
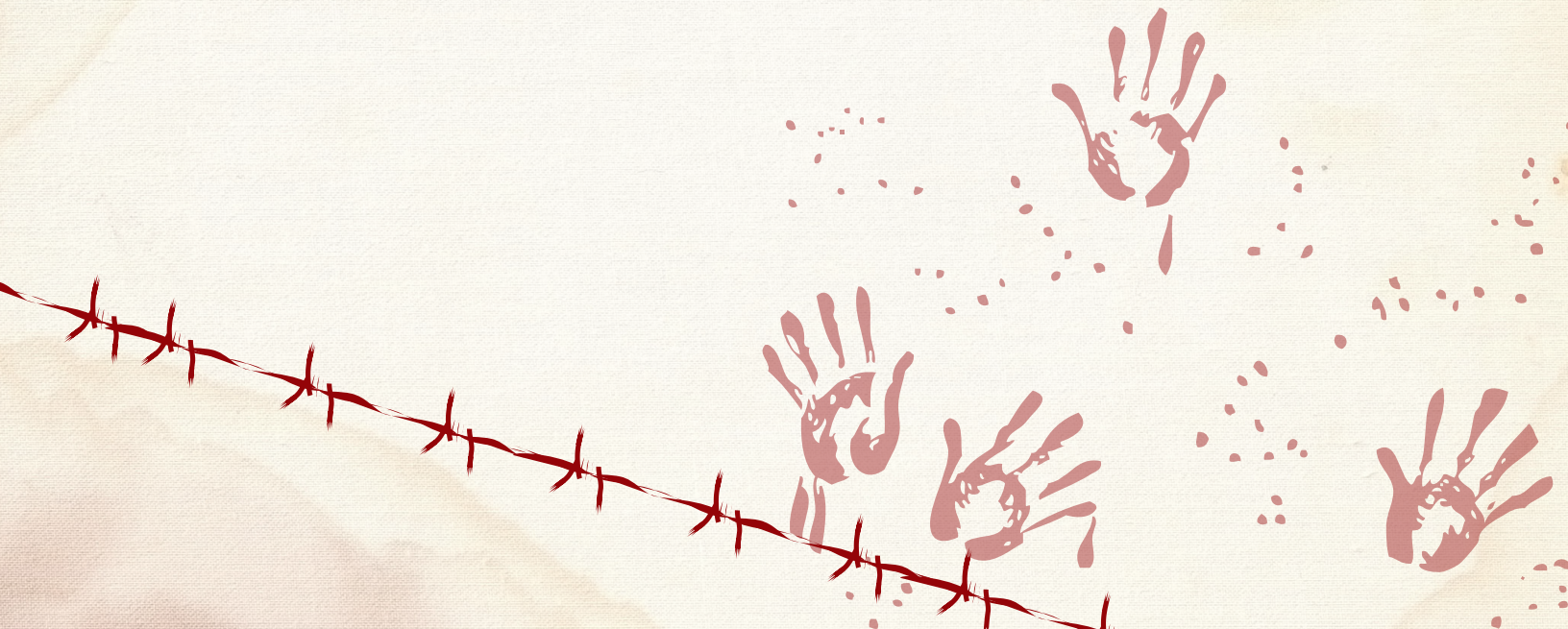
MATHCRAFT
SECURITY TECHNOLOGIES, INC.



RESPECT. DIRECT. PROTECT.

AN INDUSTRIAL SECURITY SURVIVAL GUIDE

TABLE OF CONTENTS



I. [PNNA] POLLYANNAS NEED NOT APPLY

NOTICE

WHEN IN DOUBT, DON'T LET ZOMBIES INTO YOUR CLEARED FACILITY **(DLZIYCF)**.

ZOMBIES MAY ACT LIKE THEY HAVE OFFICIAL BUSINESS ON YOUR PROPERTY, BUT DON'T LET THEM FOOL YOU! IF THEY DON'T HOLD CLEARANCES, THEY'LL PROBABLY WANDER INTO A CONTROLLED AREA OR CAUSE SOME OTHER TYPE OF SECURITY ISSUE.

IN OUR EXPERIENCE, IT'S BEST TO PRE-REGISTER THEM THROUGH THE PROPER CHANNELS. THEN, WHEN THEY ARRIVE AT YOUR FACILITY, YOU CAN SCAN THEIR GOVERNMENT-ISSUED IDENTIFICATION, COLLECT THEIR SIGNATURES (IF THEY HAVE HANDS), AND PRINT THEM BADGES. YOU CAN EVEN ASSIGN THEM SECURITY ESCORTS, IF NEEDED, BEFORE THEY GET ACCESS TO YOUR PROPERTY.

IT'S BETTER TO BE SAFE THAN SORRY.

Dear Security Officer,

In today's tumultuous industrial security environment, you can't be a Pollyanna and assume that nothing bad is ever going to happen. When it comes to industrial security, I believe in the expression, "Hope for the best and prepare for the worst."

Whether you're dealing with visitor requests for zombies or changes to the National Industrial Security Program Operating Manual (NISPOM), you have to ***respect*** the importance of your position. Every guideline serves a critical purpose. You must comply and ***direct*** your organization in strict adherence.

It's your job to ***protect*** our nation's most sensitive information and infrastructure. You must be able to perform your duties both effectively and efficiently, with this singular mission in mind.

In this text, we'll teach you more than industrial security survival techniques; we'll give you the skills to help your organization thrive.

IMO ETUK
President/CEO
MathCraft Security Technologies, Inc.

II. [WSHTF] WHEN STUFF HITS THE FAN

We have compiled five common survival scenarios that Chief Security Officers (CSOs), Chief Information Security Officers (CISOs), Facility Security Officers (FSOs), and other Security Officers are likely to experience at least once – if not several times – during their careers. Some are more extreme than others, but they all speak to situations around the time WSHTF.

If you can imagine yourself in these scenarios, you'll be more likely to recognize them quickly when they happen in real life. The sooner you can pinpoint WSHTF, the better your survival rate will be. Following each scenario, we've also framed some questions so that you can get your brain in the industrial security mindset.

See if you can envision yourself:

1. ENSNARED in a merger or acquisition.

You always thought that your large GovCon was doing well – but apparently the Board thought that it could do better. You're now in the midst of a merger with a company even larger than yours, and to make matters worse, lay-offs are just around the corner. Your security systems couldn't be more different than the new company's, and with the mountain of work in front of you, neither solution seems adequate.

How will you find freedom in the chaos... and will you stay or will you go?

2. FLAILING to stay afloat during rapid organizational growth.

When you started working at this company, it was a small GovCon with one contract. Everything ran smoothly and you knew every employee's Periodic Reinvestigation (PR) schedule by heart. Flash forward 10 years and your company now has over 10 contracts and 200 employees, and your boss just landed its biggest contract yet with a new federal client, the Department of Defense (DoD). It seems like you're about to see a 50-percent increase in your workforce – and workload. You also need to figure out the International Traffic in Arms Regulations, known as ITAR, so that you can quickly get your organization compliant.

How will you confidently comply... and increase your productivity?

3. MIRED within a data silos.

You've been working with a fast-paced, mid-sized GovCon for about a year now. It has been steadily growing ever since you started, but your requests for extra support have largely been ignored by upper management. Thanks to your ancient, paper-based systems, your newer counterparts are still struggling to learn what goes where, and when. You're the only one who knows where to look when information is needed. You'd like to take two weeks off next summer to go on a cruise, but at this rate, a real vacation from interruptive work emails and texts seems impossible.

How will you disseminate knowledge... and improve access to data?

4. OVERWORKED and overlooked.

Digital Transformation isn't a new concept in the federal space, but it seems like it is taking forever to find its way into the industrial security components of your organization. Redundant processes, manual data entry, and piles of paper fill your days, making it difficult to actually utilize your skills to make progress within your department. If it doesn't get any better soon, you're going to start looking elsewhere to make a difference.

How will you apply your acumen... and transform your daily routine?

5. GRASPING blindly for relevant, real-time data.

You've become good friends with the Resource and Portfolio Managers in your organization. They are constantly looking to you for insight on the status of security clearances – for both current employees and applicants – as well other data that is difficult to compile in a timely manner. You try to help them out when you can, but as soon as you collect the information they need, it's too old to help them out. You hate to provide pointless data, but you don't know what else to do.

How will you enlighten your coworkers ... and harness the power of your data?

III. [TBTF] TOO BIG TO FAIL

As someone in the security field, it's time for you to realize that you're TBTF. It's not just about you anymore; your organization and its employees depend on you for survival, too. Whether you created the Standard Operating Procedures (SOPs) that your department lives by or you serve as the liaison between your contract its Cognizant Security Authority (CSA), nothing runs smoothly – or at all - without your help.

- **You must respect compliance and regulatory needs.**
- **You must direct your security efforts proficiently and professionally.**
- **You must protect the individuals, information, and infrastructure that has been placed under your care.**

Survival begins with preparedness. The following seven steps will help you establish a daily routine that will make best practices inherent.

DAILY INDUSTRIAL SECURITY PREPPER CHECKLIST

1. **GET YOUR SITREP.** Log into any sites that require consistent monitoring, such as Joint Personnel Adjudication System (JPAS/DISS), for up-to-date statuses on personnel clearances, etc.

2. **BE ON THE LOOKOUT.** Check your calendar for important events, like inspections, audits, training, etc. You never want to be caught off-guard, especially when compliance is critical to everyone's success.

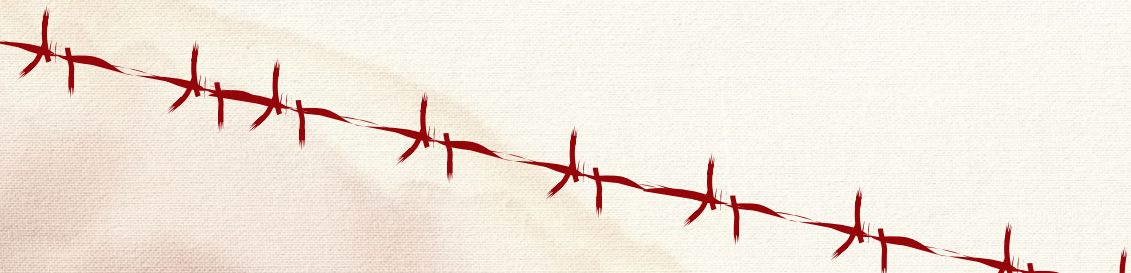
3. **SECURE THE AREA.** Take a slow stroll around your facility and Sensitive Compartmented Information Facilities (SCIFs), keeping an eye out for details like mandatory checklists, signage, physical security features, and possible security violations.

4. **GATHER INTEL.** Ask Project Managers (PMs) and other supervisors about suspicious behavior and incidents. Use this time to uncover upcoming foreign travel or foreign contact plans, as well.

5. **DEAL WITH ISSUES.** Whether you need to investigate a violation, prescribe personalized training, or suggest corrective action, it's always best to deal with problems sooner rather than later.

6. **COVER YOUR ASSETS.** Keep your data current! Carve out a block of time every day to update information regarding training, critical inventories, policies, etc. If needed, contact your CSA or Government Special Security Officer (SSO) for guidance.

7. **IMPROVE YOUR CACHE.** What can you do today to enhance your situation tomorrow? Is there a process you could automate or a paper trail you could digitize? There is no such thing as "procrastination" in your field.



IV. [TUISST] THE ULTIMATE INDUSTRIAL SECURITY SURVIVAL TOOLKIT

Every CSO, CISO, FSO, and Security Officer should have a robust and comprehensive technological toolkit. The kit should not only prep you for WSHTF; it should help you prevent panic-worthy scenarios in the first place.

We recommend a three-pronged approach when building your personalized toolkit:

Access Commander® Industrial Security Management Software

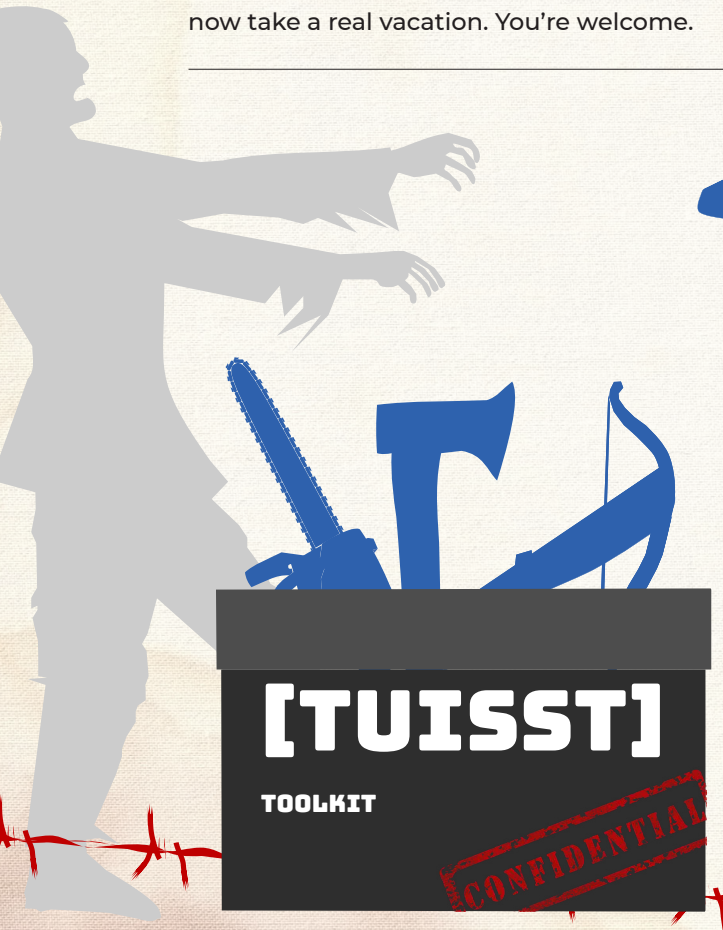
- **RESPECT** – Govern your data! Make compliance with NISPOM and other Defense Counterintelligence and Security Agency (DCSA) requirements simple and inherent. Need more? How about ad-hoc reporting, JPAS/DISS synchronization, and accountability!
- **DIRECT** – Find more freedom! Access Commander helps Security Officers manage their time more wisely with comprehensive modules and easy-to-navigate dashboards.
- **PROTECT** – Access information 24/7! Any user with the appropriate permissions can retrieve data from any computer, any time. You can now take a real vacation. You're welcome.

Portal Commander™ Employee Self-Service Platform

- **RESPECT** – Meet every deadline! Never miss a training or PR date again with dashboard-based visibility into every contract. Plus, you'll look good doing it.
- **DIRECT** – Eliminate repetitive tasks! Create automated workflows to fit any process. And, take more off your plate by getting employees involved with their own Portal Commander logins.
- **PROTECT** – Gain valuable insight! With key metrics and limitless integration possibilities, PMs and other decision makers can access the real-time data they need to make smart, timely decisions.

ViSi Commander™ Visitor Control for Cleared Facilities

- **RESPECT** – Remove bottlenecks! Avoid security lapses by pre-registering visitors, scanning Government IDs, collecting signatures, etc. Sound familiar? You get it.
- **DIRECT** – Streamline visitor management! Create a friendly, professional atmosphere with a system that is efficient and eliminates user/guard error.
- **PROTECT** – Illuminate the revolving door! Always know who is in your facility with role-based dashboards and standardized check-in/out procedures.



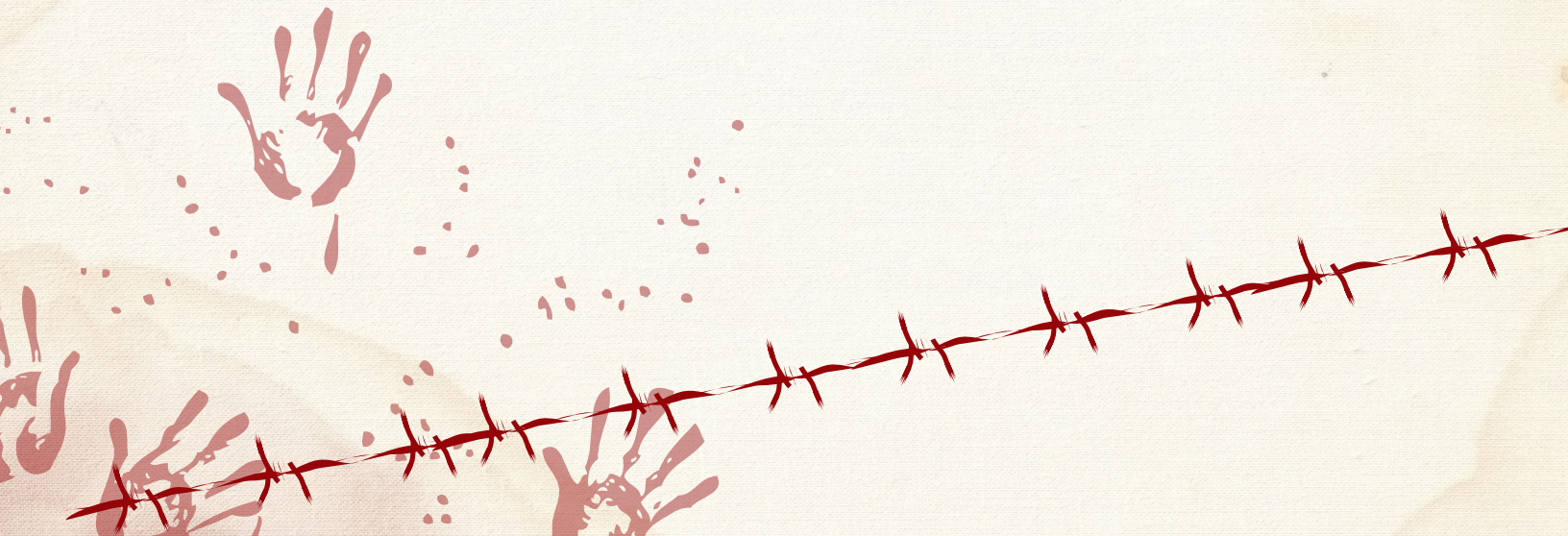
V. [YOYO] YOU'RE ON YOUR OWN

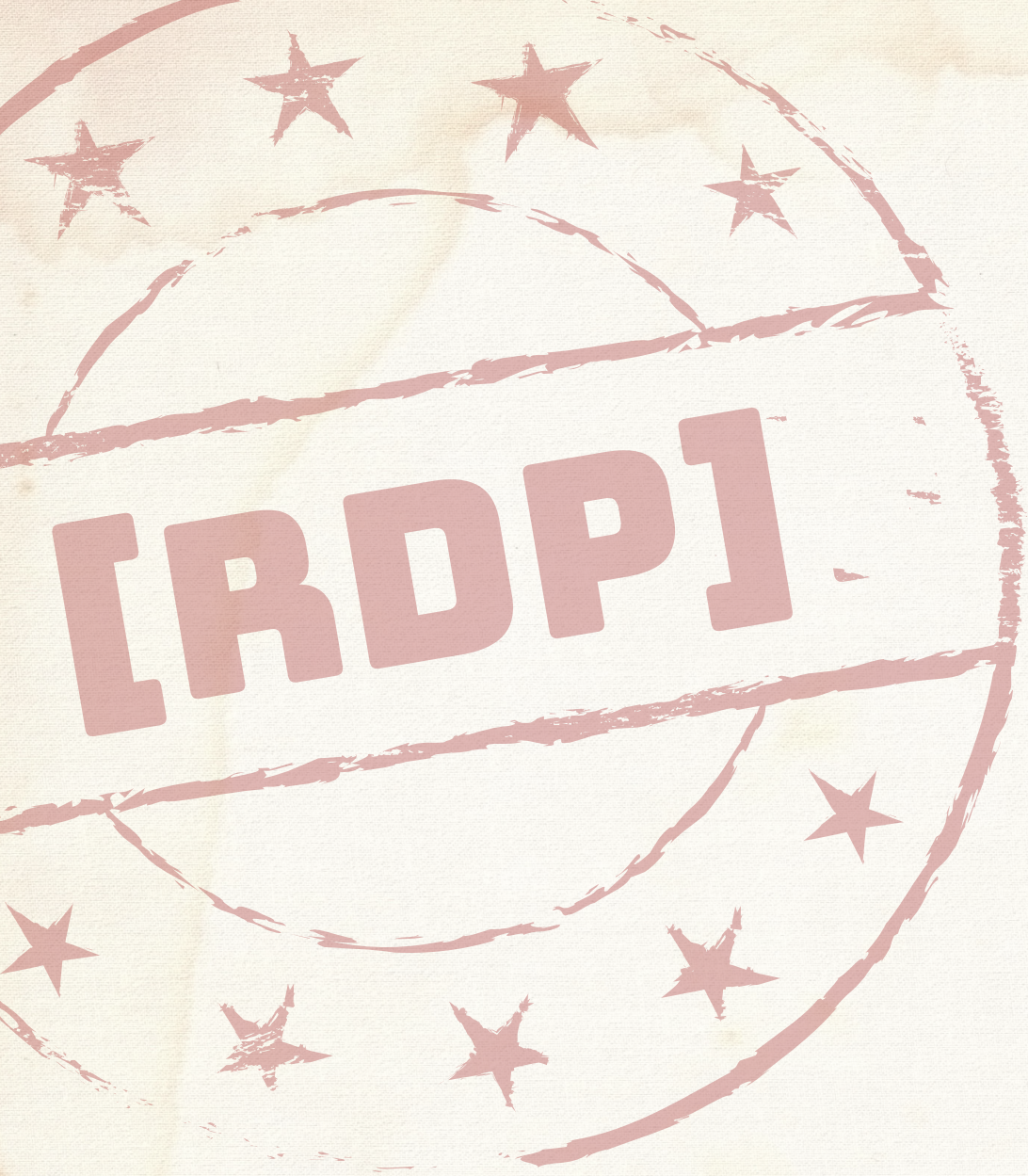
FEAR IS A FOUR-LETTER WORD.

With TUISST, MathCraft's Enterprise Security Suite, you can:

- **Find freedom in the chaos.**
- **Stay in (and earn) your rightful position.**
- **Confidently comply.**
- **Increase your productivity.**
- **Disseminate knowledge.**
- **Improve access to data.**
- **Apply your acumen.**
- **Transform your daily routine.**
- **Enlighten your coworkers.**
- **Harness the power of your data.**

YOYO, BUT MATHCRAFT CAN HELP.





MATHCRAFT
SECURITY TECHNOLOGIES, INC.

703.729.9022
www.mathcraft.com
info@mathcraft.com

44121 Harry Byrd Hwy
Suite 200
Ashburn, VA 20147