

ADVENTURE AWAITS... REPORT IT!

Know Before You Go

Submit your itinerary for unofficial foreign travel to security before you leave the country.



WHO?

Personnel who have been granted a security clearance eligibility for access to classified information or are in the process of a determination for eligibility to access classified information.



WHAT?

Unofficial foreign travel, including foreign travel conducted before, during, or after official foreign travel.



WHEN?

Report before your travel and update within 5 days after you return.



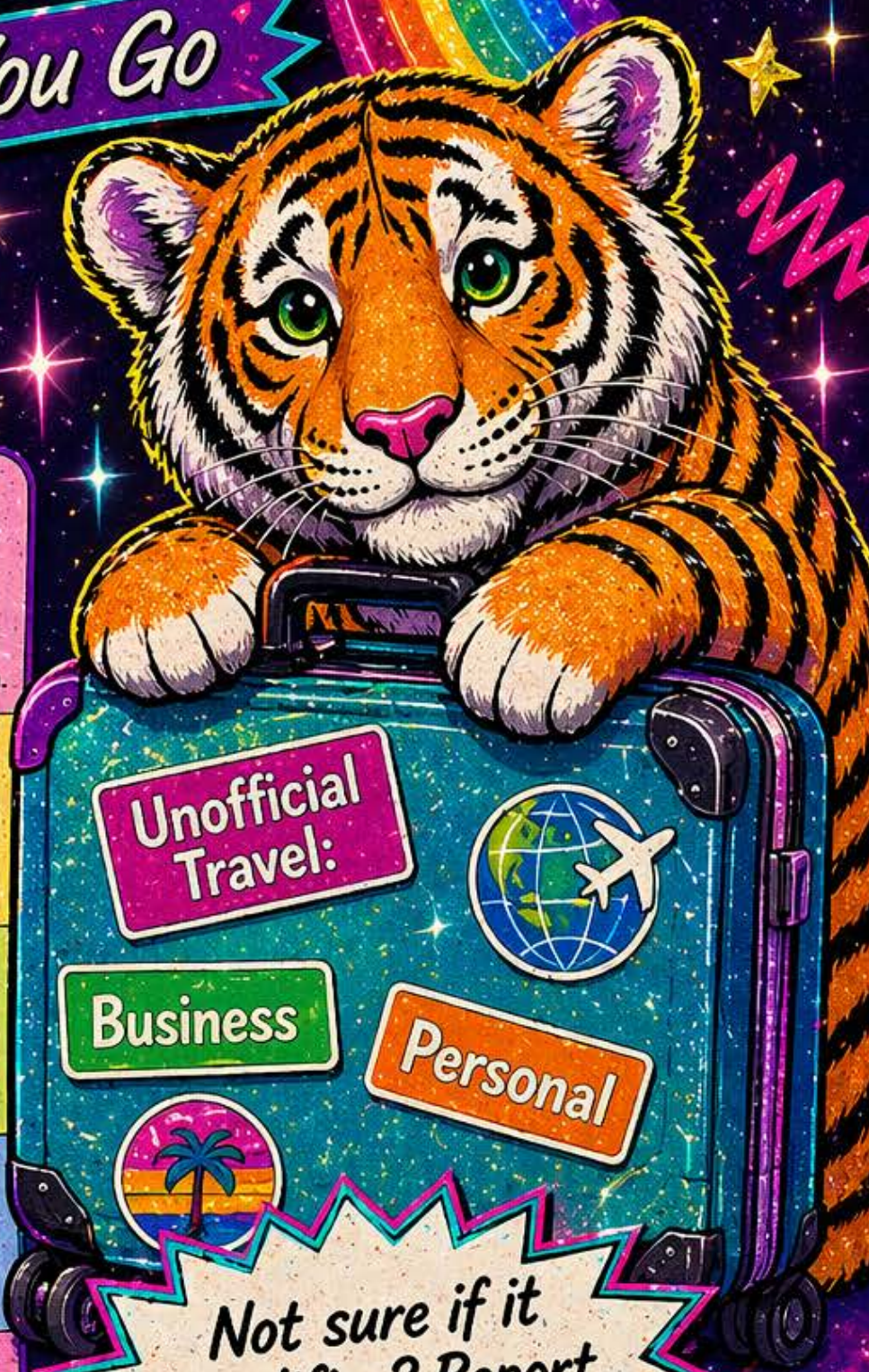
HOW?

Contact security for authorized reporting methods.



WHY?

Timely reporting helps safeguard your clearance, our information, and our national security.



Not sure if it qualifies? Report the travel anyway.



REPORT YOUR TRAVEL. PROTECT OUR MISSION.

★ Stay Aware. Stay Compliant. Stay Secure.

Adventure Awaits...Report It!

USE **AI** WITH CAUTION



**ANOTHER INCIDENT
(WAITING TO HAPPEN)**

AI with Caution

THE BIGGEST THREAT

MIGHT ALREADY

BE INSIDE

INSIDER THREAT

IT'S REAL.
IT'S SERIOUS.
IT'S PREVENTABLE.

INSIDERS
HAVE ACCESS.

ACCESS CAN
BE ABUSED.

TRUST IS
EARNED.
SECURITY IS
EVERYONE'S JOB.



WHAT YOU CAN DO:



PROTECT YOUR ACCESS.
Don't share IDs, passwords
or allow tailgating.



STAY ALERT.
Report suspicious behavior



SPEAK UP.
If something doesn't feel right,
say something.



DO YOUR PART.
Strong security starts with you

**RECOGNIZE IT.
REDUCE IT.
REPORT IT.**

**SAME ACCESS. DIFFERENT INTENT. STAY ALERT SO CRITICAL
INFORMATION STAYS SECURE.**

◀ **SECURE TODAY. PROTECT TOMORROW.** ▶

Beware the Insider Threat

Security is like ice cream; it's better with layers. Swipe your badge and keep the workplace cool and secure.



Just like you wouldn't skip the line at an ice cream truck, don't skip badging in or out. No shortcuts allowed!

Would you share your ice cream cone with a stranger? No? Then don't share your badge either! Keep your badge and your security personal.

Sharing Badges Creates Credential Risks!

Cool and Secure

COUNTERINTELLIGENCE AWARENESS



**SUSPICIOUS
ACTIVITY**



**SECURITY
BREACHES**



**ELECTRONIC
EAVESORPPING**



**FINANCIAL
MOTIVES**

CONTACT YOUR FACILITY SECURITY OFFICER

Counterintelligence Awareness

PROTECT CUI!

SAFEGUARD CONTROLLED UNCLASSIFIED INFORMATION



CUI IN THE WRONG HANDS CAN PUT NATIONAL SECURITY AT RISK!



LOCK & ENCRYPT FILES



SECURE MESSAGES & DEVICES



LIMIT ACCESS TO AUTHORIZED PERSONNEL



DESTROY & DISPOSE OF PROPERTY



THINK BEFORE YOU SHARE!

PROTECTING CUI IS EVERYONE'S RESPONSIBILITY

CUI - Safeguard CUI

So DISTRACTING...

You missed the **THREAT.**



Cute distractions can be used to bypass your security.

STAY FOCUSED. STAY SECURE.



Be aware of your surroundings.



Control access to secure areas.



Challenge unfamiliar people.



Report suspicious activity.



DON'T LET DISTRACTIONS COMPROMISE OUR SECURITY.

See it. Say it. Secure it.



INFORMATION & COMMUNICATION TECHNOLOGY

Cuteness Overload



**“IN ATLANTA
TRAFFIC’S A MESS”**

**CRIMINAL
LANE**

**CYBERSECURITY
LANE**

**“—BUT OUR CYBERSECURITY
LANES STAY CLEAR AND
SECURE”**

Cyber Lanes

**DATA DEFENSE
IS OUR DAWG PRIDE**




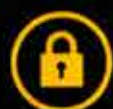


**NO INTRUDERS ALLOWED
PAST THE FIREWALL**

Dawg Pride Defense

SO DISTRACTING... YOU MISSED THE THREAT



STAY FOCUSED. STAY SECURE.

-  Be aware of your surroundings
-  Control access to secure areas
-  Challenge unfamiliar individuals
-  Report suspicious activity



Distracting

**SAFEGUARD YOUR
CLASSIFIED MATERIAL AT
ALL TIMES**

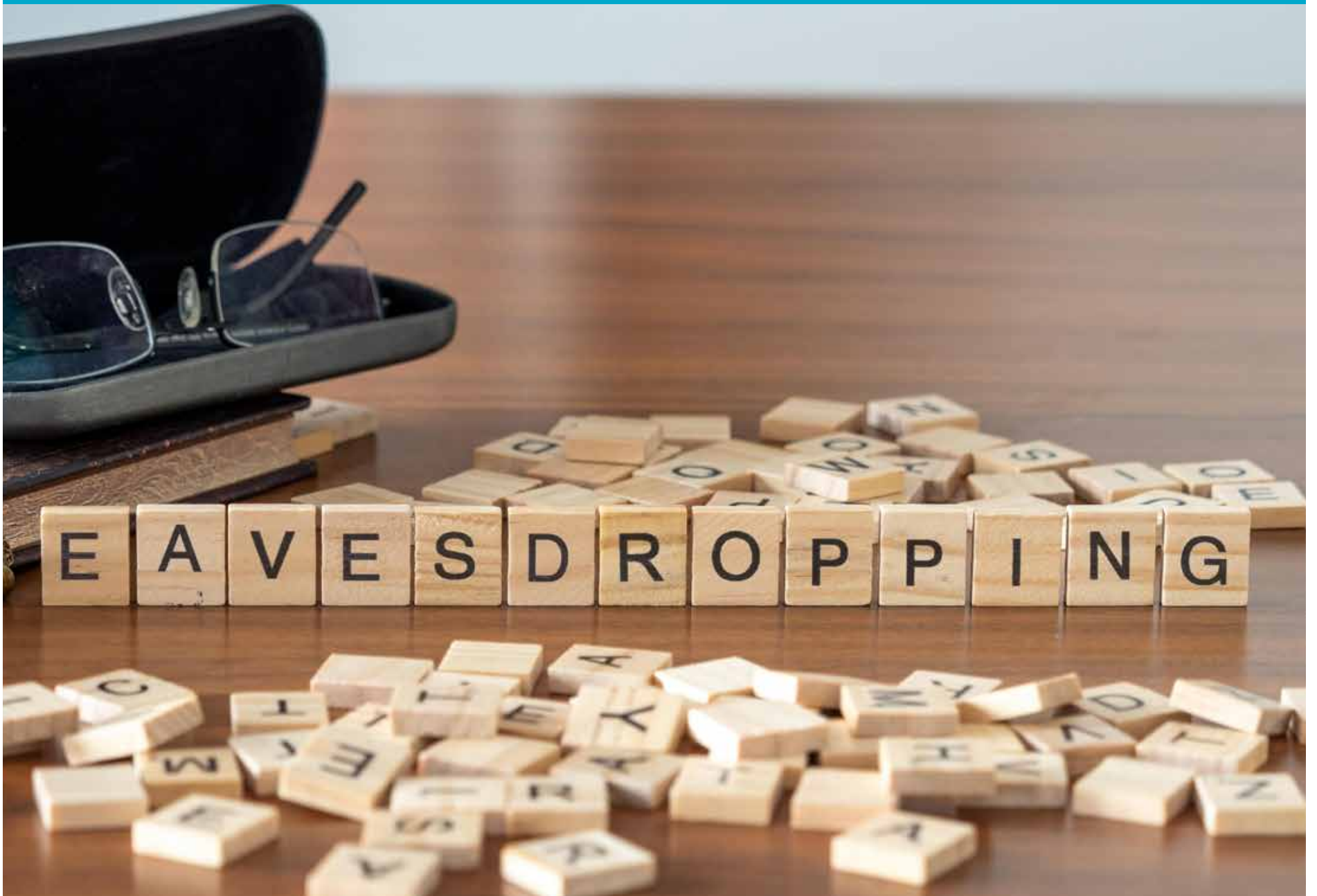
DO NOT LET IT SLIP THROUGH YOUR HANDS!

Image Microsoft



Don't Let it Slip Through Your Hands

Do you know who is listening to your conversations?



Be mindful of those around you in the workplace when discussing classified information.

Eavesdropper

How Long is Too Long to Leave a Visitor Alone?



Any Time at All.

**SIGNED IN, ESCORTED, and SUPERVISED.
Every Visitor. Every Time. No Exceptions.**

Escorting Time

DON'T FALL PREY TO PHISHING



**IF AN EMAIL BUDES YOU...
EXTERMINATE IT!**



Exterminate

HELLO
Spring

IT'S A
GREAT
TIME
TO
GROW GOOD
SECURITY HABITS



Growing Security Habits

**IT'S ME,
HI,
I'M THE PROBLEM,
IT'S ME.**

-The Insider Threat



**They may not sing it out loud,
but all the signs are there.**

Recognize and report suspicious activity.



I'm the Problem

INSIDER THREAT AWARENESS

“The Threat Isn’t Just Outside... It’s Within.”

What is an Insider Threat?

An employee, contractor, or trusted individual who misuses authorized access — intentionally or unintentionally — to harm systems, data, or operations.

Signs of Betrayal:

- ◆ Unusual Access to sensitive data.
- ◆ Large File Downloads or Transfers.
- ◆ Access Outside Assigned Role.
- ◆ Odd Working Hours.
- ◆ Bypassing Security Controls.

Choose Your Allegiance:



The Malicious Insider
◆ The Traitor



The Negligent Insider
◆ The Unwitting Pawn



The Compromised Insider
◆ The Controlled Asset

Guard the Realm:

- Follow Least Privilege Access.
- Protect Credentials.
- Protect Credentials.
- Secure Your Workstation.
- Be Alert to Phishing & Social Engineering.
- Report Suspicious Activity Immediately.

REPORT SUSPICIOUS ACTIVITY

Report concerns to:

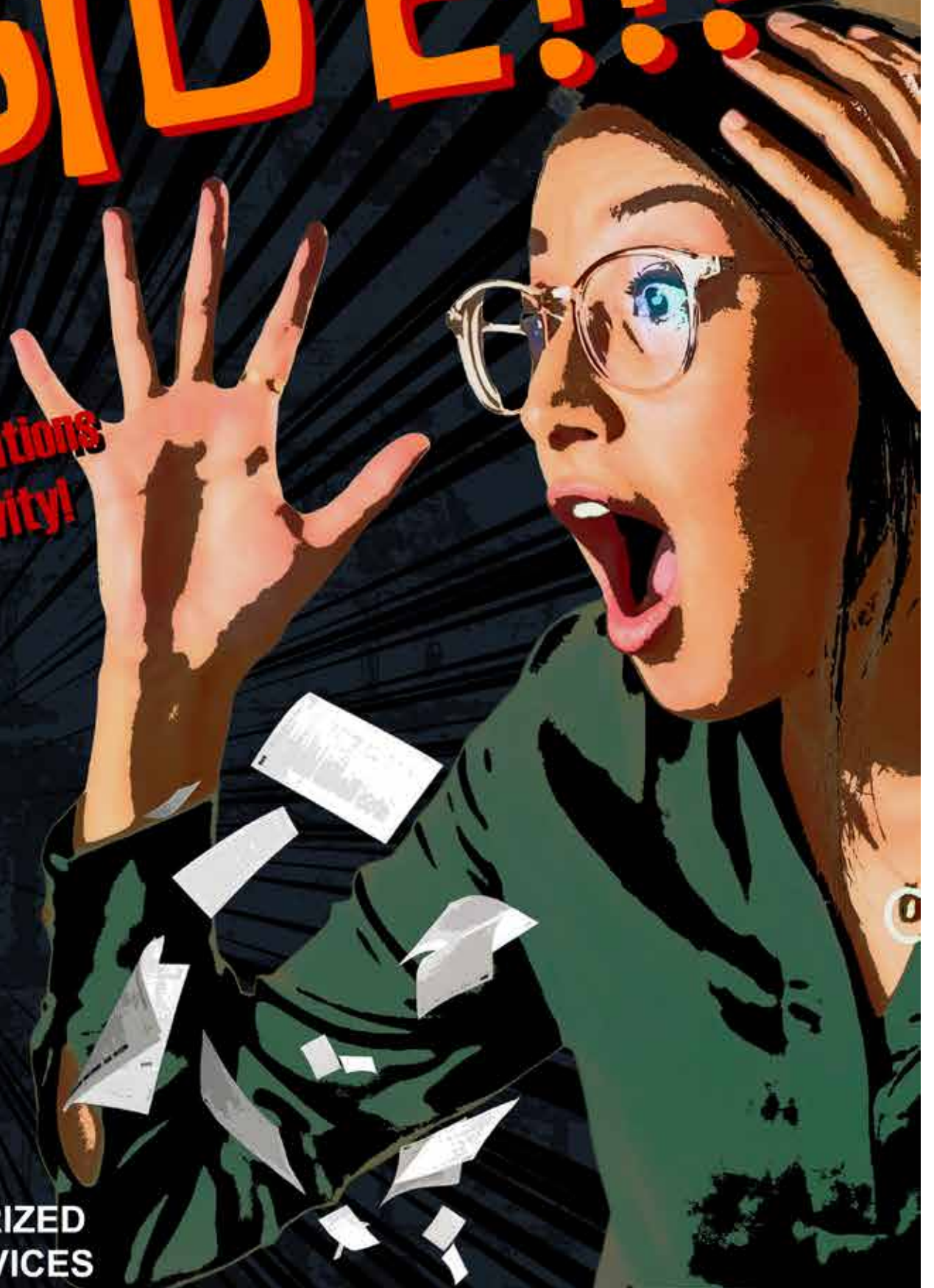
- Insider Threat Program Senior Official (ITPSO)
- Facility Security Officer (FSO)



IT CAME FROM...

INSIDE!!!

Stop the threat
from within.
Report security violations
& suspicious activity!



KEEP UNAUTHORIZED
ELECTRONIC DEVICES
OUT OF CLASSIFIED AREAS



OPEN

BEWARE
of the
INSIDER
THREAT!



It Came From Inside



KNOW WHERE TO HAVE CLASSIFIED DISCUSSIONS

AUTHORIZED

- ✓ SCIF
- ✓ CERTIFIED OPEN-STORAGE AREA
- ✓ OFFICIAL CLASSIFIED MEETING
- ✓ SIPRNET
- ✓ LIMITED AREA'S (LA)
- ✓ VAULT TYPE ROOMS (VTR'S)
- ✓ ENTERPRISE SECURE NETWORK (ESN)
- ✓ SPECIAL ACCESS PROGRAM FACILITY (SAPF)

WHEN IN DOUBT, ASK YOUR FSO.

To learn more, consider joining



Know Where to have Classified Discussions

Good security is like good ice cream: Layer it up, keep it cool and enjoy peace of mind!



Strong Passwords = Sweet Protection!

Don't let your passwords melt under pressure! Use a mix of uppercase, lowercase, numbers, and special characters. The longer, the better—just like your favorite sundae!

Beware of Phishing Cones!

Not all ice cream offers are sweet—some are just scams! If you get an email promising free treats, check the sender and avoid clicking on suspicious links. Phishers love to scoop up your data!

Two-Factor Authentication = Double Scoop Security!

Why settle for one scoop when you can have two? Add an extra layer of security with 2FA and keep your accounts safe from sticky fingers!

BONUS SPRINKLES:

- Don't share your passwords—even if someone offers you extra sprinkles!
- Always verify the source of emails, texts, or offers before you take a bite!
- Update your software regularly to keep your cone fresh and secure!

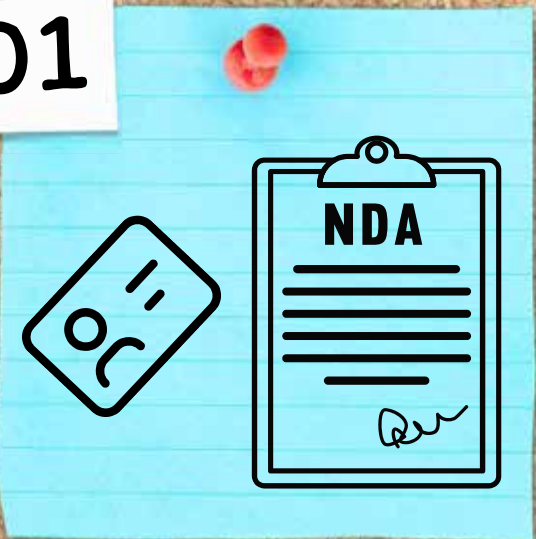
Layer It Up



Safeguarding CLASSIFIED INFORMATION



01



Accessing

1. Eligibility Determination at the correct access level
2. Need to know
3. Signed SF-312

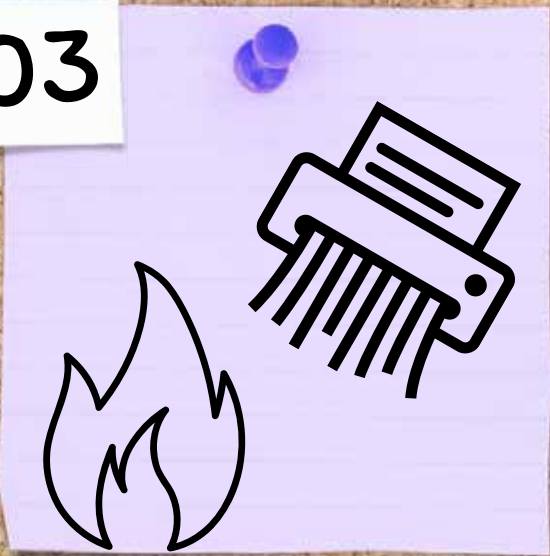
Protecting

- Only store in GSA-approved security containers
- Do not disclose to anyone who does not have the proper access
- Do not leave information unattended



02

03



Disposal

- Return all information to USG at contract conclusion
- Only use approved methods to destroy information when appropriate

Making Safeguarding Stick

Multi-factor authentication is like a bouncer:



One ID is
good...

Two is better.



MFA

**Security may seem excessive
until it's not enough.**

*Think you can
outsmart me?*

**Never
underestimate the
determination of
someone with
ample time on
their side.**

Mischief Squirrel

YOUR WORKPLACE PRESENTS

INSIDER THREATS CAN BE
INTENTIONAL OR
UNINTENTIONAL

BE ON THE LOOKOUT FOR
POTENTIAL RISK INDICATORS

REPORT SUSPICIOUS
ACTIVITIES

THEY WALK AMONG US.

INSIDER THREAT

STARRING

EDWARD SNOWDEN - PETER ZUCCARELLI - ALDRICH AMES
ROBERT HANSSEN - JOHN WALKER

COMING SOON

TALK TO YOUR ITPSO TO LEARN MORE

Now Showing: Insider Threat



INSIDER THREAT — AWARENESS —



PROTECT OUR ORGANIZATION FROM WITHIN

WHAT IS AN INSIDER THREAT?

An insider threat comes from within—people you trust who misuse their access to harm our business, data, or reputation.

Intentional or accidental,
the damage is real.



TYPES OF INSIDER THREATS



MALICIOUS INSIDER

Intent on—or sabotage



NEGLIGENT INSIDER

Careless actions that put us at risk



COMPROMISED INSIDER

Account taken over by external threats

HOW YOU CAN PROTECT THE FAMILY



RESPECT THE CODE:

Follow access rules at least privilege.



GUARD YOUR CREDENTIALS:

Never share your passwords.



LOCK THE DOOR:

Secure your workstation when away.



TRUST NO ONE BLINDLY.

Be cautious with emails, attachments



REPORT SUSPICIOUS ACTIVITY

Speak up—loyalty protects.



COMMON WARNING SIGNS



Unusual Access to sensitive data



Large Downloads of files or reports



Access Outside Role or normal duties



Odd Hours or after-hours activity



Ignoring Security Rules or bypassing controls

IF YOU SEE SOMETHING, SAY SOMETHING.

REPORT CONCERNS TO:



INSIDER THREAT PROGRAM SENIOR OFFICIAL (ITPSO)



FACILITY SECURITY OFFICER (FSO)



“SECURITY IS EVERYONE’S RESPONSIBILITY.
PROTECT THE FAMILY.”

Protect Our Organization From Within

Follow procedures
Prevent compromise



PROTECT
WHAT YOU'RE
TRUSTED WITH

Protect What You're Trusted With

To maintain your clearance, keep your clearance sweet by following the Reporting Requirements!



- **Allegiance to the U.S.:** Your loyalty to the country is the base of your sundae. Without it, the whole thing melts!
- **Foreign Influence:** Don't let foreign sprinkles ruin your dessert. Report any foreign connections that could affect your judgment.
- **Foreign Preference:** Choosing another country's toppings over your own? That's a no-go. Stick to the home recipe!
- **Sexual Behavior:** Keep it sweet and appropriate. No questionable toppings here!
- **Personal Conduct:** Integrity is the whipped cream on your sundae—without it, everything falls apart!
- **Financial Considerations:** Don't let debt melt your security. Report financial troubles before they become sticky situations.
- **Alcohol Consumption:** A little ice cream float is fine, but overindulgence could spill your clearance.
- **Drug Involvement:** Drugs are like freezer burn—they'll ruin your sundae fast. Stay clean to keep your clearance sweet.
- **Psychological Conditions:** Everyone deserves a solid scoop. Seek help if needed and keep your sundae secure.
- **Criminal Conduct:** Crime is like dropping your cone—it's messy and ruins everything. Stay on the right side of the law!
- **Handling Protected Information:** Don't let classified sprinkles fall into the wrong hands. Keep them secure and confidential.
- **Outside Activities:** Side gigs are fine but make sure they don't add sour toppings to your sundae of security.
- **Use of IT Systems:** Treat your IT systems like the cherry on top—handle them responsibly, or the whole sundae could collapse!

Sweet Tips for Reporting:

- **Transparency is Key!** Always report issues honestly. It's how we keep the sundae intact.
- **Don't Hide the Sprinkles!** Even minor issues can affect your clearance. Report them early to avoid trouble.
- **Share the Recipe!** If you see something concerning, speak up—it helps everyone enjoy their own secure sundae.

Reporting Requirements

SECURITY AWARENESS



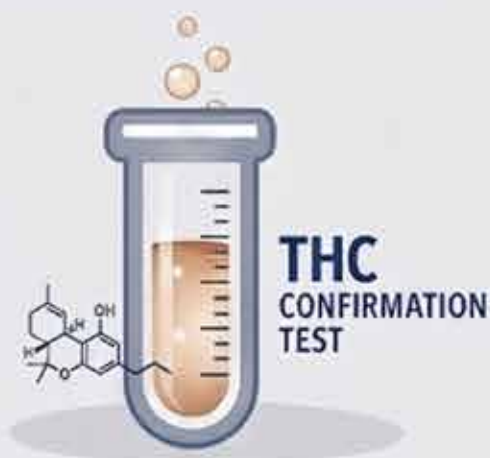
Hemp & CBD Products



No ingestible
Hemp & CBD



Labels Cannot
Be Trusted



Positive Drug Test
= Clearance Risk

AVOID THE CLEARANCE RISK

Security Awareness

SECURITY IS A JOURNEY, NOT A DESTINATION.

CONTINUOUS EVALUATION



1. FIVE-YEAR
PVQ SUBMISSION



2. TIMELY SELF
REPORTING



3. EFFECTIVE
INSIDER THREAT
MONITORING

STAY CURRENT, STAY TRUSTED.

Security is a Journey

Security Starts With You.

**Know the threats.
Follow the process.
Stay informed.**



Security Starts

SILLY MASCOT



SERIOUS SECURITY

Silly Mascot

An illustration of a green crocodile lying in a swampy environment. The crocodile is positioned in the lower half of the frame, facing left, with its mouth open showing sharp teeth. It is surrounded by green bushes and reeds. In the background, there are several trees with green foliage and hanging moss, set against a warm, yellowish-orange sky. The text "WATCH OUT FOR TAIL-GATORS" is overlaid in the center of the image in a bold, white, sans-serif font.

**WATCH OUT FOR
TAIL-GATORS**

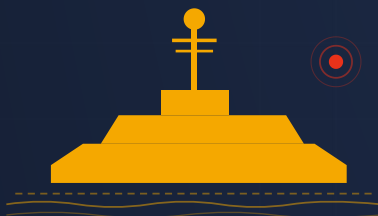
Tailgators

133

A FIELD MANUAL FOR THE INBOX

THREE THINGS OUR ROBOTS DO. YOU SHOULD TOO.

Every SimIS platform already embodies a security principle most people forget at their desks. The discipline is already in the room. Apply it.



RIVER SCOUT · SAMS

// 01

RECON BEFORE ENGAGEMENT.

Our autonomous platforms survey, identify, and verify before advancing into uncertain water. The same logic at your desk: hover the link, read the URL, verify the sender. Then advance.

FIELD APPLICATION – PHISHING · LOOKALIKE DOMAINS · VENDOR FRAUD



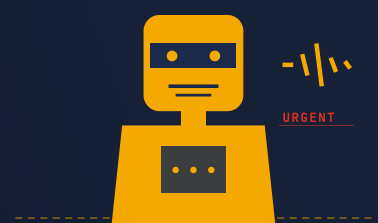
HTT · ROBOTIC HUMAN-TYPE TARGETS

// 02

EVERY SHOT IS LOGGED.

HTT records every hit and miss. LOMAH data improves training, not punishment. Your clicks, logins, and transfers are telemetry too – the SOC watches the way HTT watches.

FIELD APPLICATION – AUDIT TRAILS · INSIDER RISK · OBSERVABILITY



ADRT · DE-ESCALATION ROBOTIC TRAINER

// 03

DE-ESCALATE BEFORE YOU CLICK.

ADRT trains officers to recognize manufactured urgency and respond instead of react. Phishing exploits the same heat. Pause. Verify. Then act.

FIELD APPLICATION – URGENCY-BASED SOCIAL ENGINEERING · BEC

MODEL THE FUTURE.
SECURE THE ENTERPRISE.
STARTS AT YOUR DESK.



IGNORING OBVIOUS INDICATORS OR WARNINGS...



...CAN HAVE SERIOUS
CONSEQUENCES!

Be Aware of Your Surroundings and
Always Report Suspicious Activity!

Contact your Counterintelligence Representative for additional information and to report suspicious contacts and activity.

LOCKHEED MARTIN 

Warning Indicators



Don't Be Your Organizations Weakest Link!

**Remember to Take Your
Annual Security Training**



Weakest Link

**Do You Know Who
Is LISTENING To Your
CONVERSATIONS?**



**Be mindful of those around you
in the workplace when discussing
classified information.**

Who is Listening

can you spot the insider threat?



it could be anyone...

report suspicious activity to your FSO

Who's IT?

SECURING AN OSA?

5S IT!



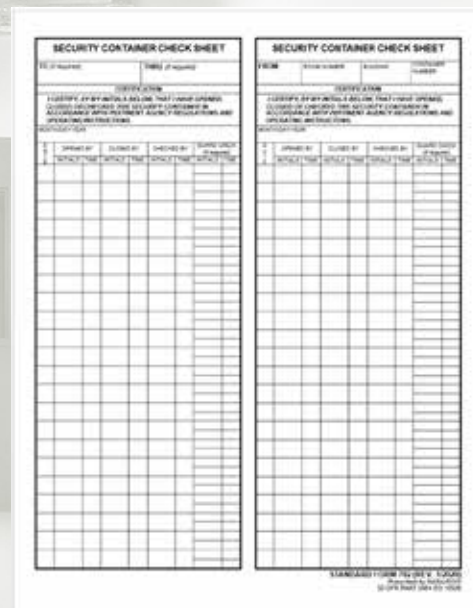
Swipe & Arm



Spin



Swipe & Test Door



Sign



Spin Again

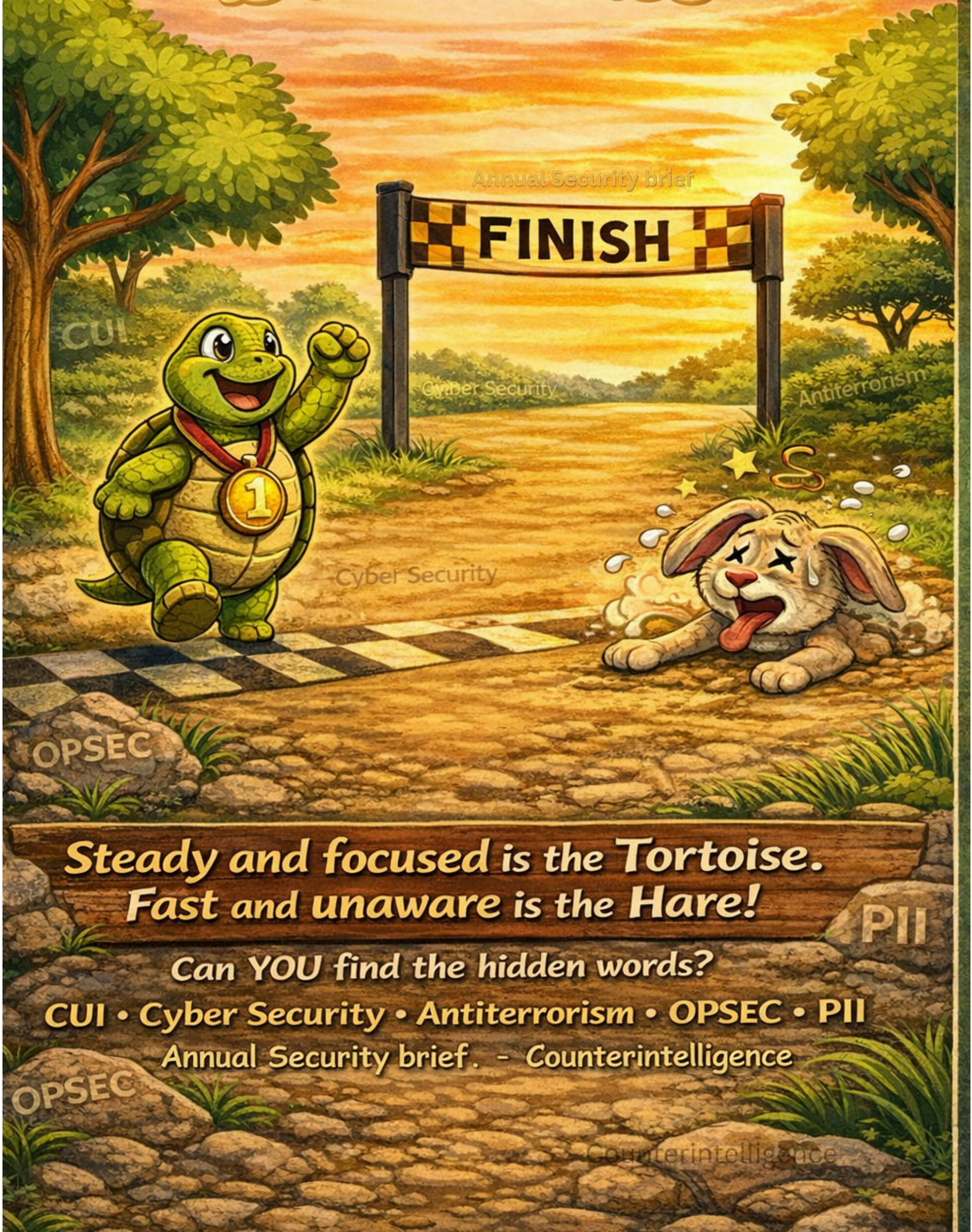
A good process produces good results.

-Nick Saban

Questions, please contact your Program Security Representative!

5S the OSA

Annual Training is not a race



***Steady and focused is the Tortoise.
Fast and unaware is the Hare!***

Can YOU find the hidden words?

CUI • Cyber Security • Antiterrorism • OPSEC • PII

Annual Security brief. - Counterintelligence

Annual Training is Not a Race



**Strong Security Starts Here
Protecting America –
From Atlanta to Los Angeles**

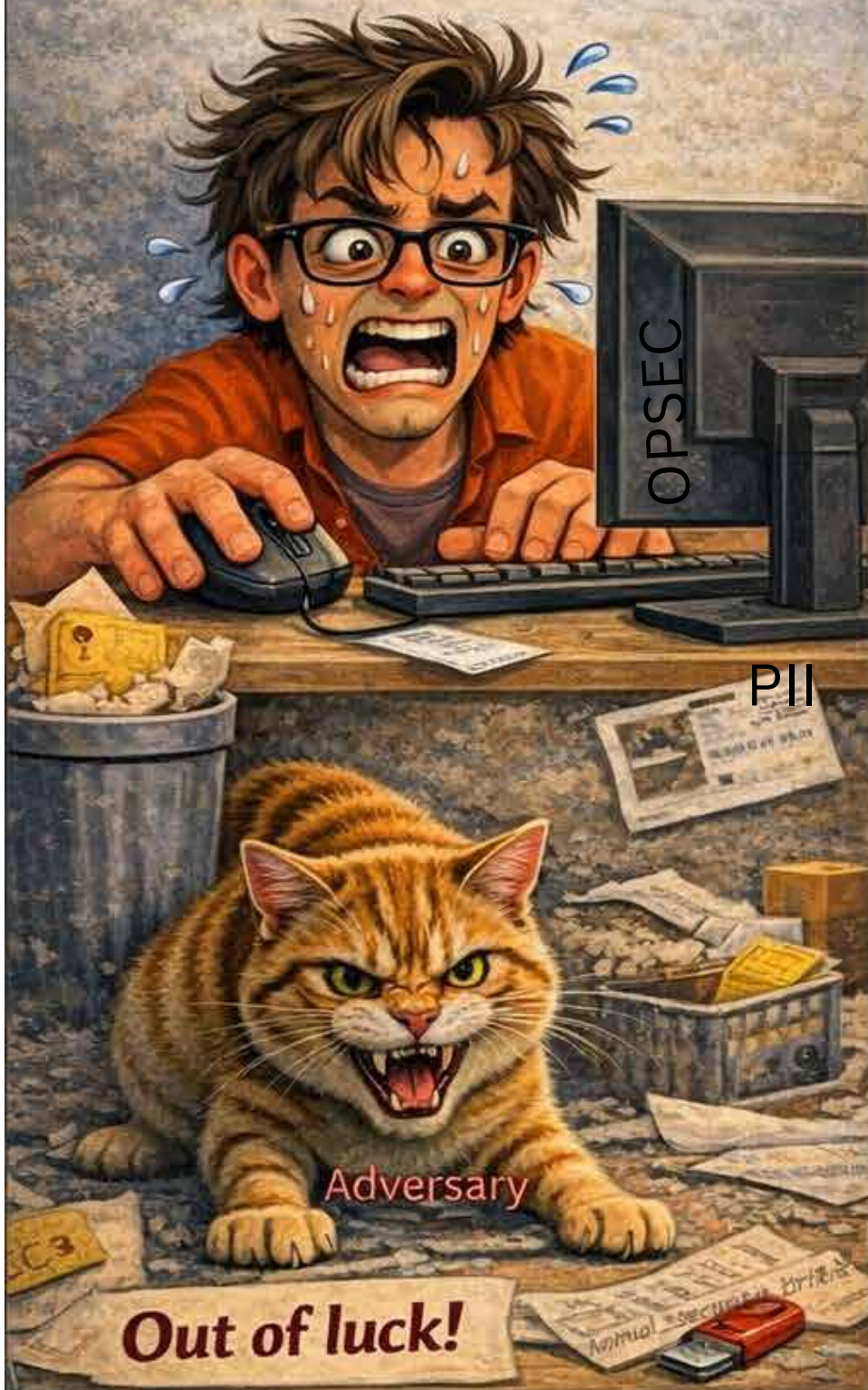


Atlanta to LA

Be Smart with Annual Training!

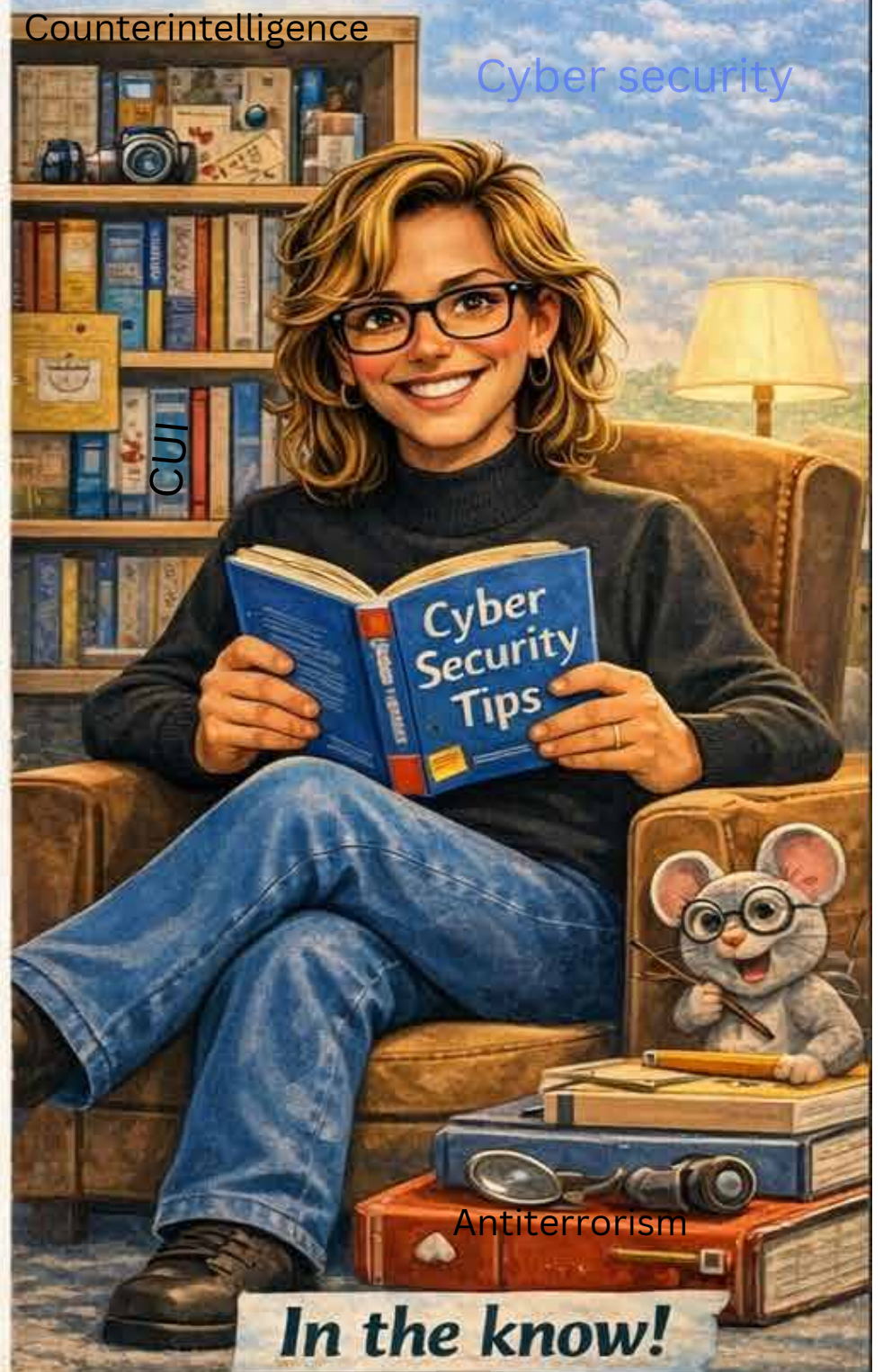
Poor Bill...

Clicked too fast...
Missed the facts!



Awesome Jerry...

Took her time...
Learned just fine!



Can you spy annual training?



CUI, Cyber security, Counterintelligence, PII,
Annual security brief, OPSEC, Antiterrorism

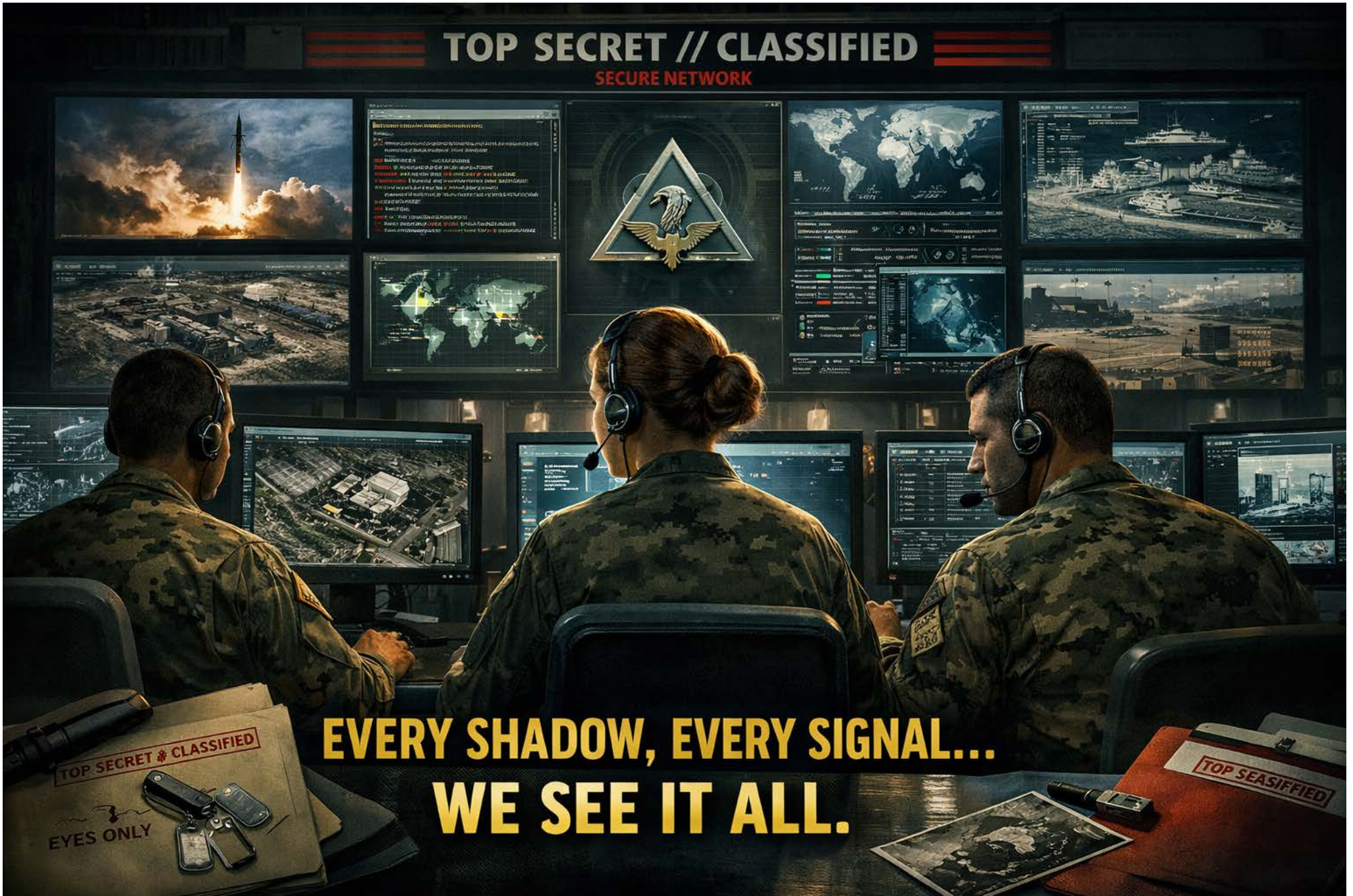
Be Smart With Annual Training

"SWEET AS A GEORGIA PEACH, TOUGH AS
FIREWALL-HACKERS....."



"CAN'T TAKE A BITE OUT OF ME"

Bite My Peach



Cyber Ops Center

Data Breachy not so

Peachy

keep cybercriminals out by
using strong secure passwords,
keep your software updated, and
be on the lookout for phishing emails.



Data Breachy

CYBERSECURITY AWARENESS

DATA TRAVELS FAR.

ONCE IT LEAVES,
YOU LOSE CONTROL.



Data Loss

IF THEY CAN GET IN

ANYONE CAN



Unauthorized access doesn't start with force. **It starts with one missed step.**

Control site entry
Badge in/Badge out
Challenge unknown individuals
Secure doors, gates, and restricted areas
Report suspicious activity
Follow all access control procedures

EVERYONE PLAYS A ROLE

SEE IT. QUESTION IT. **STOP IT.**

Dino Baby

★ **KEEP CUI PROTECTED** ★



STAY OUT OF THE DOGHOUSE!



ENCRYPTION



LOCK UP FILES



ESCORT VISITORS

Doghouse

Don't be Bill. Be Jerry!

Poor **Bill** clicked too fast through his annual training. He missed all the tips, reminders, & warnings! 😞

Jerry paid attention! He loved the refresh and learned of new threats. Knowing the knooks and crannies helped him avoid the new pet adversary.

Don't be Bill. Be Jerry!



Can you spy annual training?
CUI, Cyber security, Counterintelligence, PII,
Annual security brief, OPSEC, Antiterrorism.

Don't be Bill, Be Jerry

HUNT DOWN THE THREATS!

REPORT TO SECURITY!

ESPIONAGE



SUSPICIOUS CONTACTS



INSIDER THREATS



SEAD 3 REPORTABLES:



FOREIGN TRAVEL



FINANCIAL CONCERNS



MISUSE IT SYSTEMS



ADVERSE BEHAVIOR

HIT



SCORE

012300

HIGH SCORE

050000

Duck Hunt

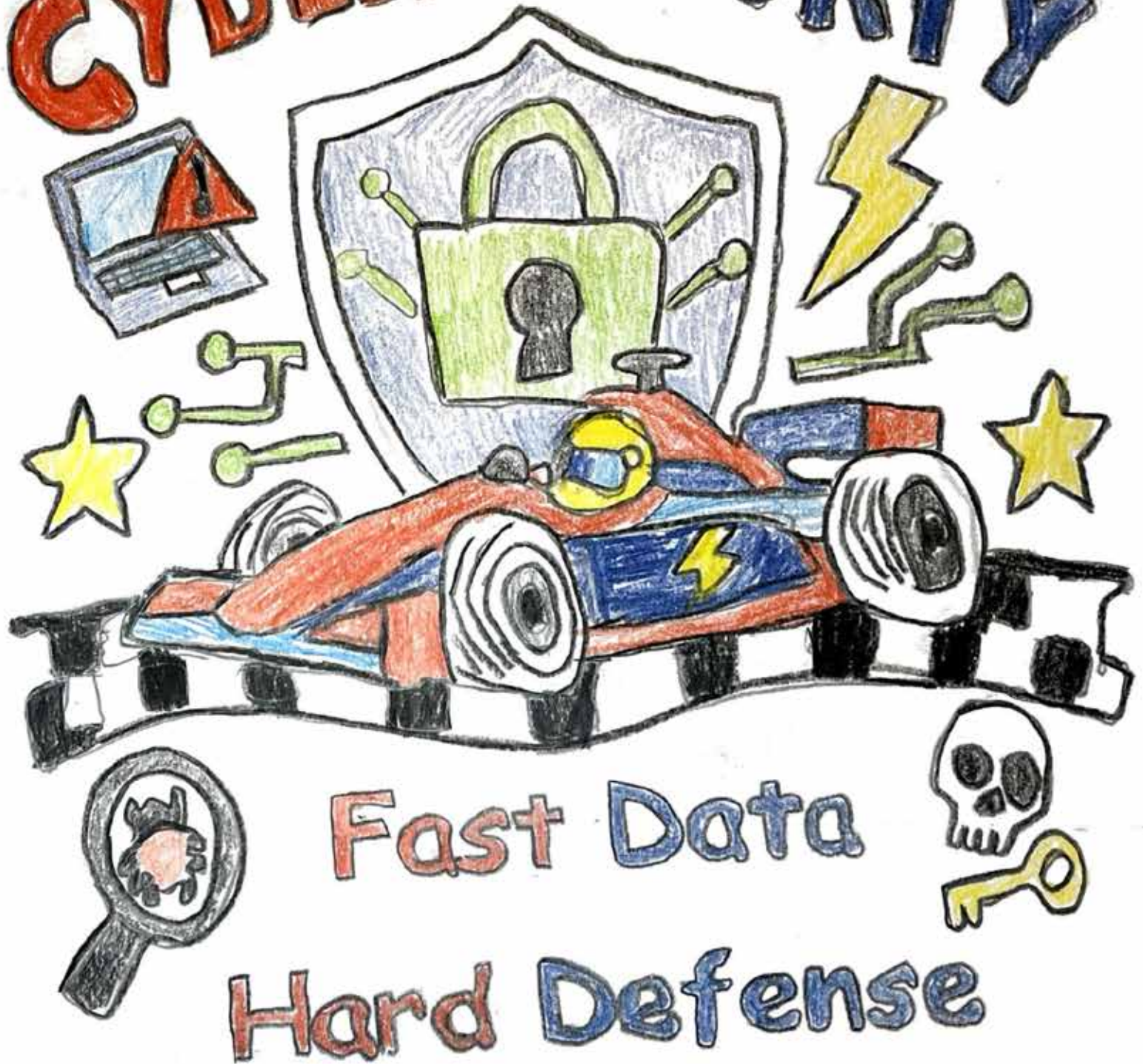
**PROTECT THE INFORMATION YOU
ARE ENTRUSTED WITH**



YOU NEVER KNOW WHO IS WATCHING!

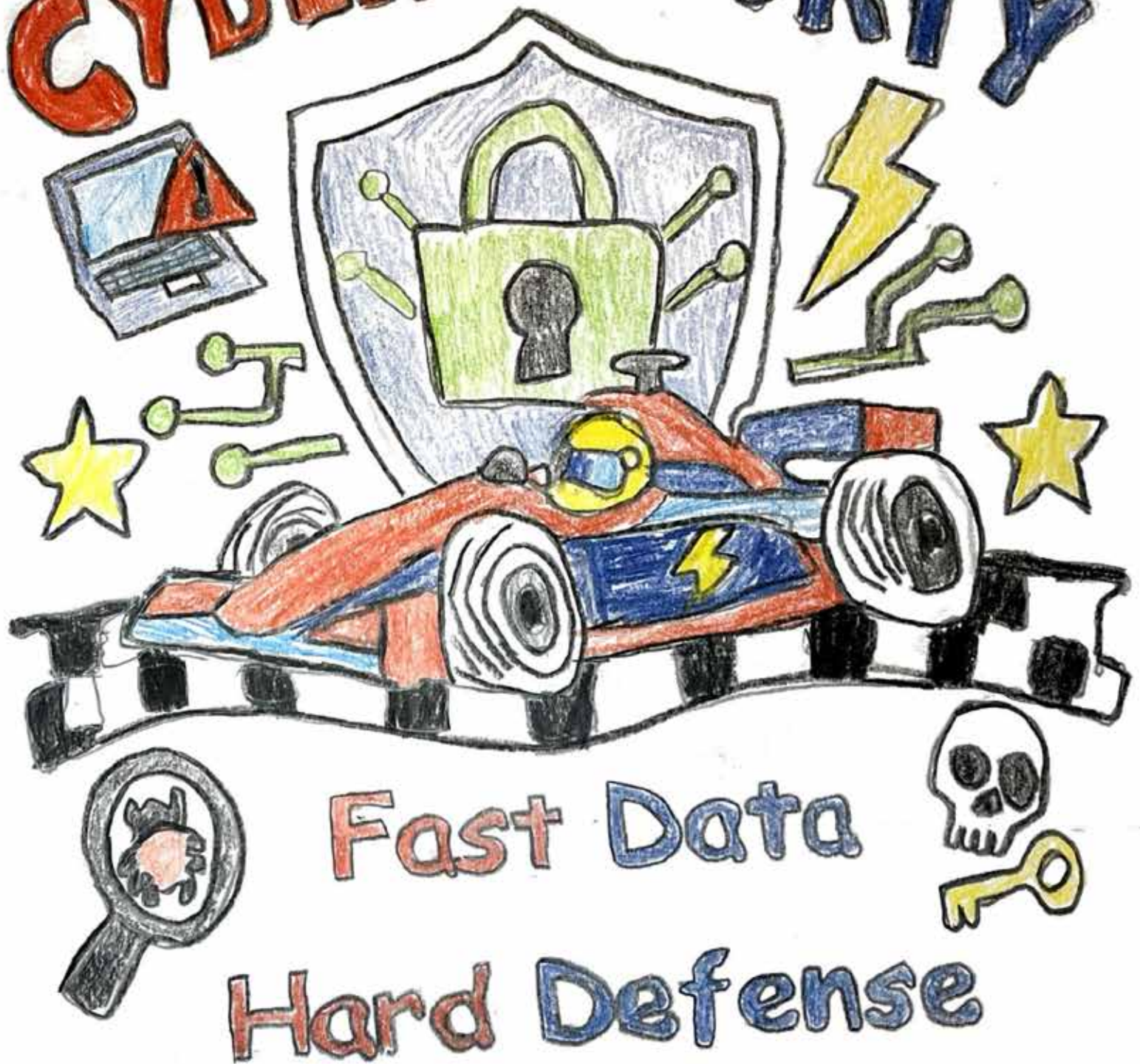
Entrusted Eye

CYBER SECURITY



Fast Data

CYBER SECURITY



Foreign Travel Reporting

FSO HOURLY RATES

\$75.00/hr - Standard W-2 rate. Includes patiently providing the 32 CFR reference explaining, once again, why the FSO must be a W-2 employee.

\$100.00/hr - If we're going to have a meeting about why the room upgrade still isn't complete.

\$100.00/hr - If your questions could already be answered had the FSO been provided a DD Form 254, as required.

\$125.00/hr - If we're going to discuss why I cannot do things the way your previous FSO did (please consult the latest version of 32 CFR, things change).

\$150.00/hr - If you ask how long it will take for someone to get a clearance (short answer: longer than you want).

\$175.00/hr - If you ask why a security function is taking so long to complete.

\$200.00/hr - If you ask questions that are already clearly answered in the annual training you definitely attended.

\$250.00/hr - If you ask me to obtain an employee clearance without justification, documentation, or physics defying timelines.

\$275.00/hr - If we're discussing an issue that should have been reported months ago but somehow wasn't.

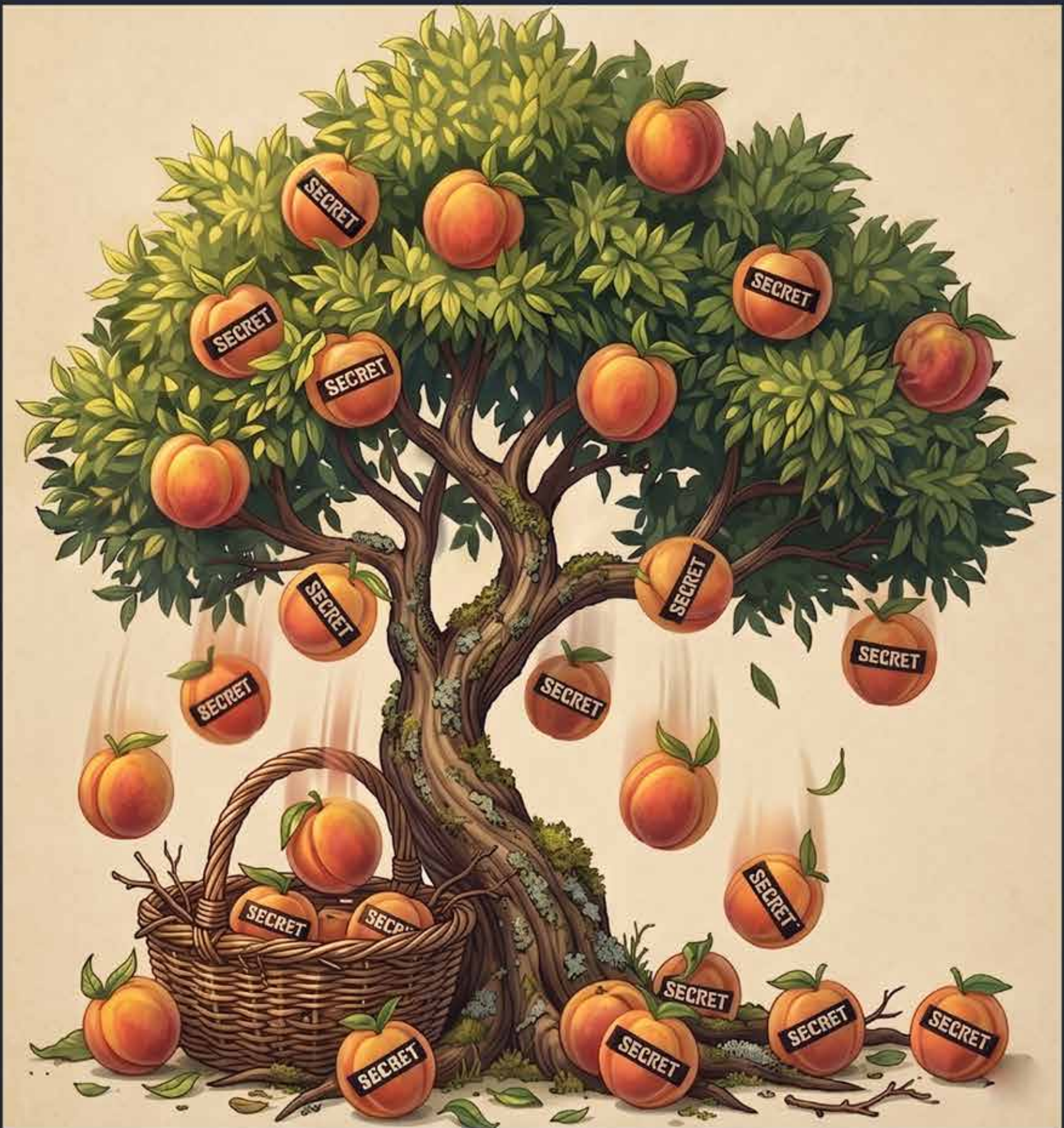
\$300.00/hr - If you'd like me to relax security procedures because of your title, role, or confidence level.

\$350.00/hr - If you want me to call the DISS Help Desk to check on an employee's clearance status after I already spoke to them yesterday, and nothing has changed

The role of the Facility Security Officer, along with company security policies and procedures, cannot be overstated. These exist to protect you, the company, and all of us from very uncomfortable conversations later.

FSO Hourly Rates

**Really love your secrets,
wanna shake your tree.**



**Practice Good
Operations Security**

Georgia Peach Tree



**KEEP
YOUR DATA
LOCKED
TIGHTER
THAN:
GRANDMA'S
PEACH
COBBLER
RECIPE**



Grandmas Peach Cobbler

HIDDEN HAZARDS



This image looks calm. *It is not.*

ONE OF THEM IS A BULL

Threats don't announce themselves.
COMPLACENCY GIVES THEM ACCESS.

Hidden Hazards

NCMS Poster Contest Entry Form

Entry Deadline: May 1st

Note: An entry form must accompany each Poster Competition entry. All entries must be submitted via the designated submission tool by a Chapter Chair or the CCL Team.

I hereby consent to the release, modification, publication, and distribution of the poster competition entry described below submitted by me to the NCMS Poster Competition. I also consent to the use of my name and organization in connection herewith.

I hereby pledge to NCMS that my agency/company will continue for a period of one year the distribution of the items entered on the same terms as before the contest and will not increase the price charged for the item(s) because of an item winning an NCMS award.

I declare that, to the best of my knowledge, said poster is rightfully submitted by me to NCMS with all necessary authority, that permission has been obtained by me for use of any original work in this entry, and I further confirm that I am free to disclose or make use of the said competition entry in my possession which now passes to NCMS. I declare that there are no commitments or restrictions on the competition entry that would constitute a conflict of interest between NCMS, any other organization, and me. Said entry is submitted to NCMS for the limited purpose of providing security education to its members.

I understand that when entering any posters for consideration in this competition, it may result in further distribution and as such, I hereby grant NCMS permission to add the NCMS logo, if necessary, then publish and distribute the said item as a NCMS security education and training product. This may be accomplished by placing the entry on the NCMS website or by mass distribution. This is done to promote the product for its membership and other interested parties and will be granted for an indefinite duration of time. Further, it is agreed that NCMS will incur the expense of editing, modifying, printing, and distribution of entry for said purposes. Further, NCMS may use my name and likeness on or in connection with any promotional material published by it without further compensation to me.

As the owner of, or the holder of, the poster competition entry described as follows, I hereby agree to accept the conditions above:

Category:	<input checked="" type="checkbox"/> Chapter	<input type="checkbox"/> Professional
Entry File Name: <i>Must be provided by the Chapter chair</i>	<i>Example: 26CBAYNewDesign1</i> New Design	
Entry Poster Name:	<i>Example: NCMS is Awesome</i> Insider Threat	
Printed Name of Sponsor / Entrant:	Diane Partridge	
Signature of Sponsor / Entrant:	<i>Diane Partridge</i>	
Sponsoring NCMS Chapter Name / Org:	Texas Gulf Coast CH14	
Chapter Chair Signature:	<i>Ruby Reynolds</i>	

Insider Threat

INSIDER THREAT AWARENESS

TRUST... BUT VERIFY

Familiar doesn't mean safe



Insider Threat



“Was I really talking that loud?”

An insider threat, particularly the risk of someone within your organization overhearing your conversations, poses significant dangers, primarily related to data breaches, intellectual property theft, and potential sabotage or financial fraud. These threats can stem from malicious actors within the company, those who unintentionally leak sensitive information, or those who are coerced or tricked into sharing confidential data.

Insider Threats

**DON'T BE
IN THE DARK
ABOUT SECURITY**

IAP
WORLD SERVICES, INC.



Left In the Dark

Looks Cute Bites Faster

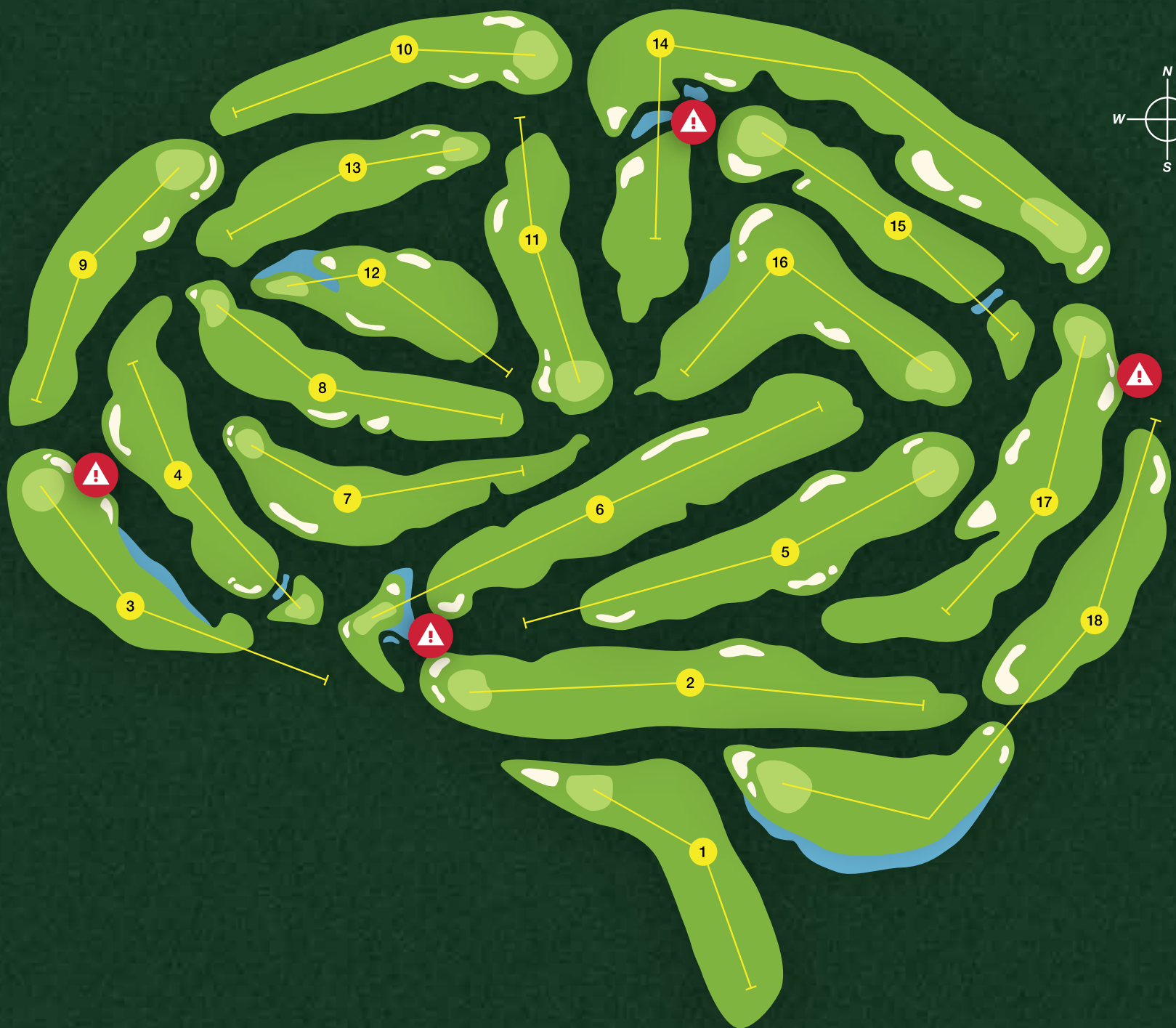
**Report
Suspicious
Activity**



Looks Cute Bites Faster

BECOME
MASTERS
OF
BEST PRACTICES

STAY ON PAR WITH GOOD SECURITY



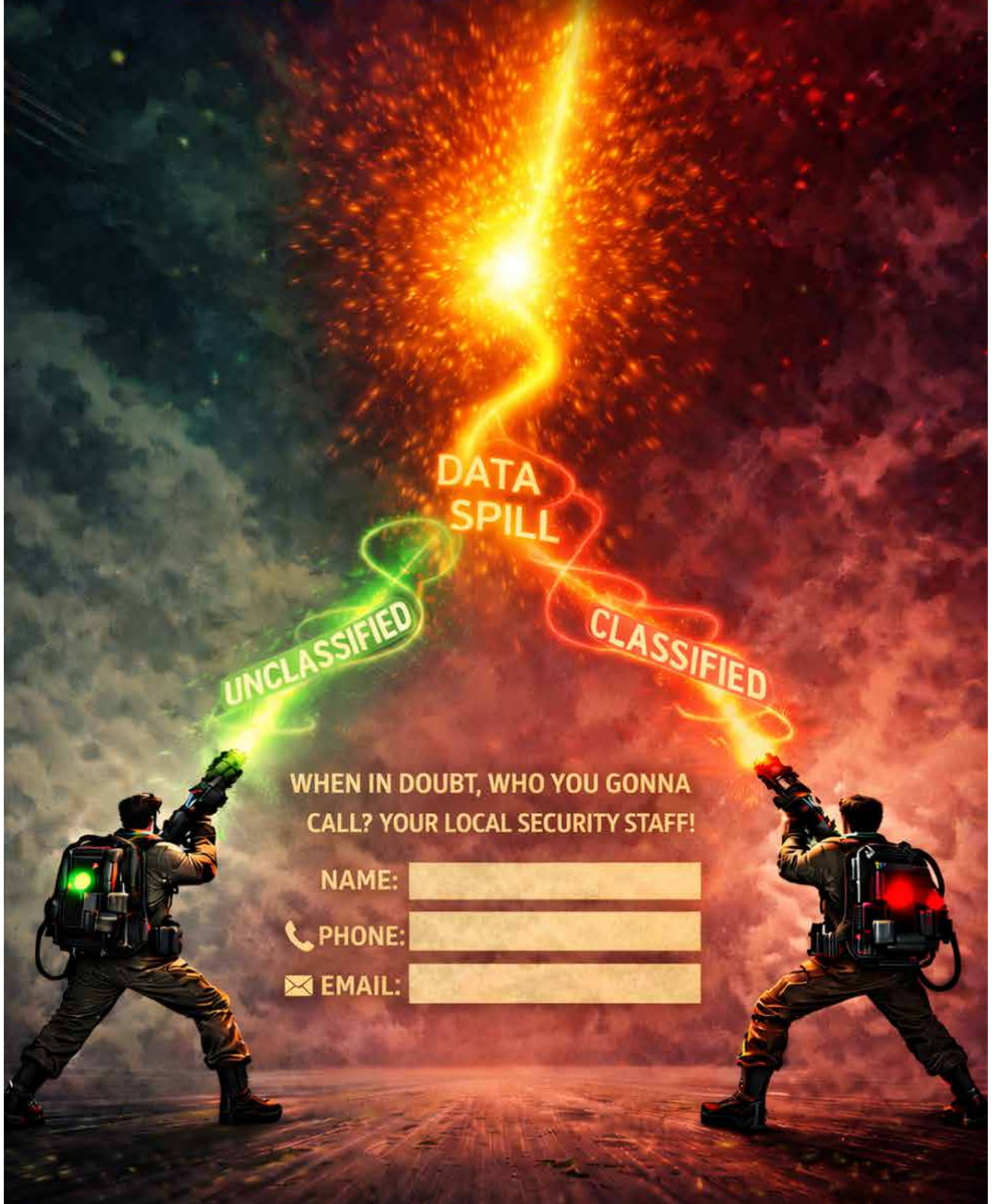
HAZARDS TO KEEP TOP OF MIND

- ⚠ Weak Passwords
- ⚠ Public Wi-Fi
- ⚠ Unlocked devices and information
- ⚠ Untrusted email links and attachments



Mentorship

NEVER CROSS THE STREAMS BETWEEN UNCLASSIFIED AND CLASSIFIED INFORMATION



WHEN IN DOUBT, WHO YOU GONNA
CALL? YOUR LOCAL SECURITY STAFF!

NAME:

PHONE:

EMAIL:

Never Cross the Streams

**LIKE THE BULLDOGS IN
STANFORD STADIUM--
STRONG, PROTECT YOUR TURF**

AND....



NEVER LET HACKERS SCORE

Never Let Hackers Score

UNEXPECTED NORTHERN LIGHTS

Protect our People
Protect our Facility

Badge In/Badge Out
Report Suspicious
Activity Immediately
Challenge Unknown
Individuals
Follow All Access
Control Procedures

REINFORCE THE IDEA THAT THREATS CAN EMERGE

ANYWHERE

Northern Lights in Ohio

Me and my Dad Fishing



**Not all fishing is
innocent...don't catch
the bait!**



Not all Fishing is Innocent

Don't Let Your Security Go Off the Rails



Re-Train Every Year



Off the Rails

OPERATION: SEAD 3 REPORT!

REPORT SECURITY RISKS BEFORE THEY CAUSE A BUZZER!

FINANCIAL
TROUBLES!



FOREIGN
CONTACTS!

BUZZZ!

SUBSTANCE
ABUSE!



FOREIGN
CONTACTS!

UNUSUAL
TRAVEL!



REPORT CONCERNS NOW!

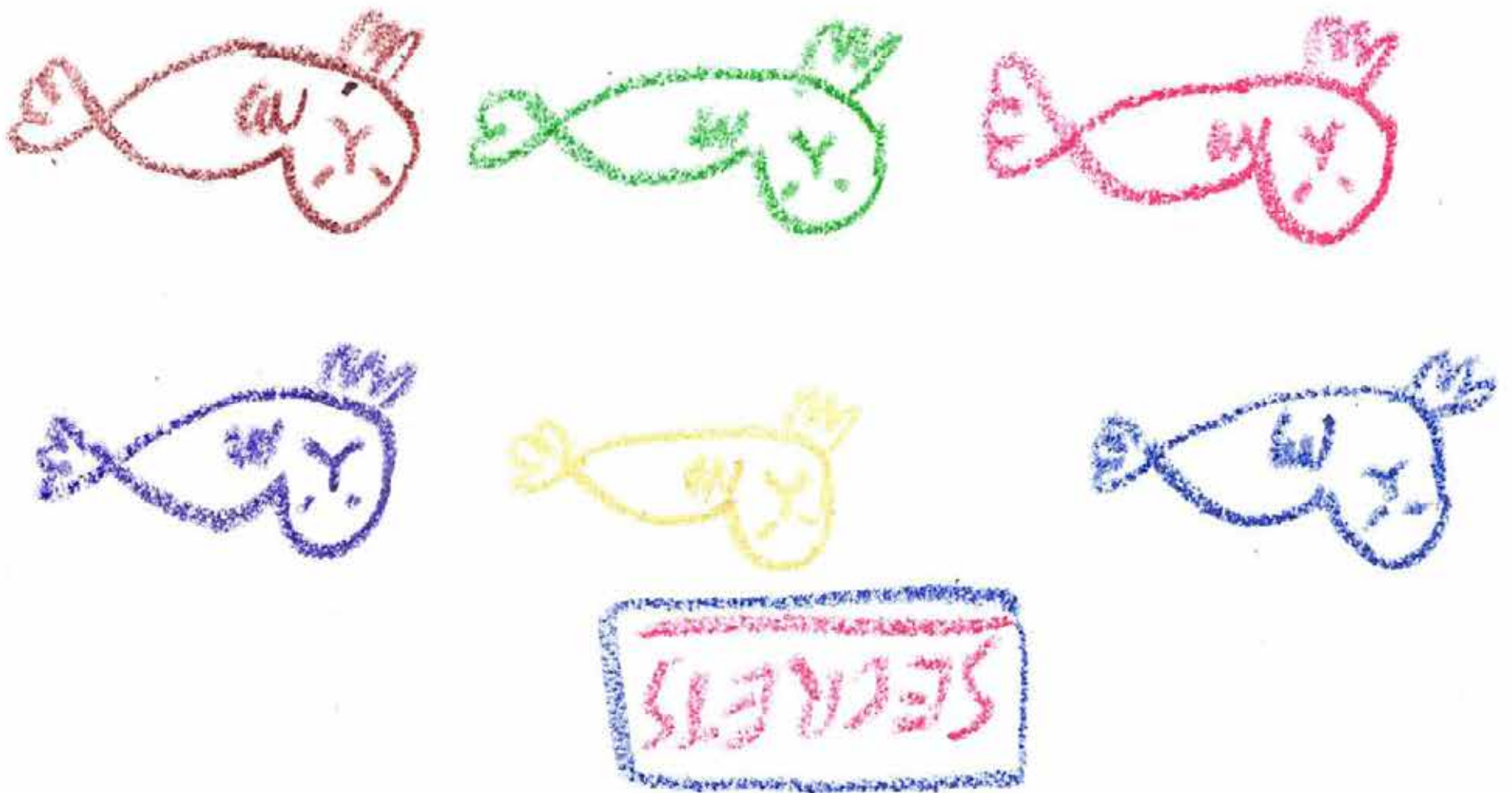
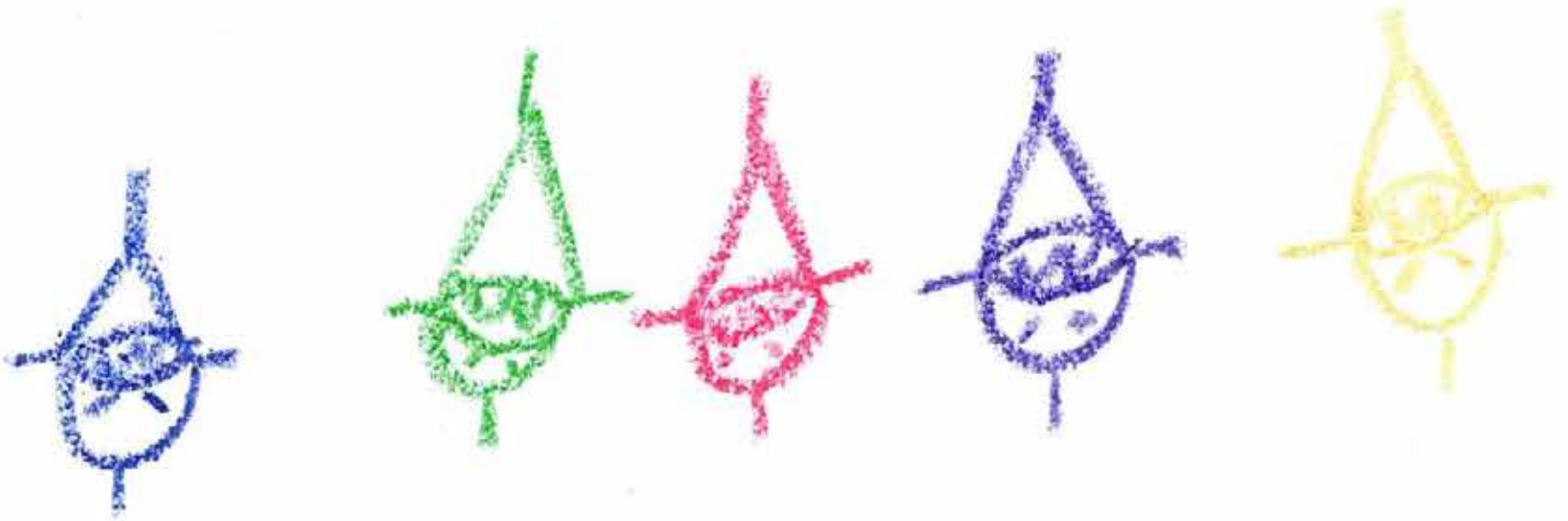
CALL YOUR SECURITY OFFICE!

- ✓ ANY FOREIGN CONTACTS?
- ✓ FINANCIAL ISSUES?
- ✓ SUSPICIOUS BEHAVIOR?



Operation SEAD 3

OPSEC is important!
to protect your secrets
You don't need SEALS



OPSEC Seals



**STRONG PASSWORDS
GROW BETTER THAN
PEACHES
IN GEORGIA
HEAT**

Peach Passwords

CYBERSECURITY AWARENESS

NOT EVERYTHING YOU **CATCH** IS SAFE

That “**phish**” might cost you everything.



Phishing Trap

A woman with a large afro hairstyle and a shocked expression covers her mouth with both hands. In the background, a hooded figure in a dark blue hoodie is visible against a dark background with pink and purple horizontal stripes. A speech bubble is positioned above the woman's head.

“I think I just gave away my personal information.”

It is crucial to avoid sharing personal information online, such as your name, address, phone number, or Social Security number, with individuals you don't know personally. This is because such information can be misused by scammers, identity thieves, or other malicious actors for various harmful purposes.

PII Security

STEP UP YOUR SECURITY GAME!

DON'T GET PHISHED!

WATCH OUT FOR SUSPICIOUS EMAILS & LINKS!



SAFEGUARD YOUR DATA!

PROTECT SENSITIVE INFO & BACK UP YOUR FILES!



STRONG PASSWORDS HIT A HOME RUN!



P@SSwOrd123!

USE COMPLEX & UNIQUE PASSWORDS

KEEP YOUR EYE ON THE BALL!

BEWARE OF SOCIAL ENGINEERING SCAMS!



PLAY IT SAFE ONLINE!



AVOID MALICIOUS WEBSITES

REPORT SUSPICIOUS ACTIVITY!

IF YOU SEE SOMETHING, SAY SOMETHING!

STAY CYBER AWARE!

DON'T GET CAUGHT OFF GUARD!

- ★ THINK BEFORE YOU CLICK!
- ★ KEEP SOFTWARE UP TO DATE!
- ★ LOCK DOWN YOUR DEVICES!



Play It Safe

SECURITY IS BUILT IN LAYERS.



Power of Layers

Security on Your Mind



Protect What's Inside.



Protect What's Inside

Keep Your Security On Track



Re-Train Every Year



Retrain

ARE YOU WILLING

TO PLAY

RUSSIAN ROULETTE

WITH YOUR

ELECTRONICS?

ONE WRONG SCAN...



**COULD STEAL
YOUR DATA**



**INSTALL
MALWARE**



**ACCESS YOUR
ACCOUNTS**



**COMPROMISE
YOUR PRIVACY**



**THINK BEFORE YOU SCAN.
TRY YOUR LUCK.**

Russian Roulette QR

THE SEAD 3 TRAIL

Don't Get Stranded by Security Violations!

AVOID OCCURRENCES
of SECURITY DANGER!

Follow SEAD 3 and keep
your mission moving forward!



☠ DANGEROUS OCCURRENCE #1 ☠



Mishandling Sensitive Info

You left classified information unsecured.

☠ DANGEROUS OCCURRENCE #2 ☠



Weak Passwords

Using "123456" made your account easy pickings for outlaws.

☠ DANGEROUS OCCURRENCE #3 ☠



Ignoring Phishing Emails

By engaging with a phishing email, you were ambushed by cyber rustlers.

☠ DANGEROUS OCCURRENCE #4 ☠



Foreign Contacts Not Reported

A contact with a foreign national snuck up on your party. You let it go unreported.

☠ DANGEROUS OCCURRENCE #5 ☠



Misusing Govt Systems

You misused government resources for personal matters.

☠ DANGEROUS OCCURRENCE #6 ☠



Failure To Complete Required Training

You failed to complete mandatory security training.

FOLLOW THE TRAIL TO BETTER SECURITY!



[Continue on to complete your training.]

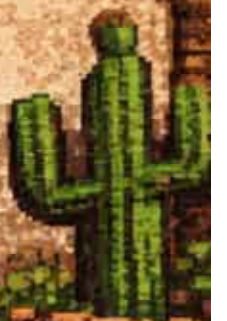


[Report security concerns promptly.]

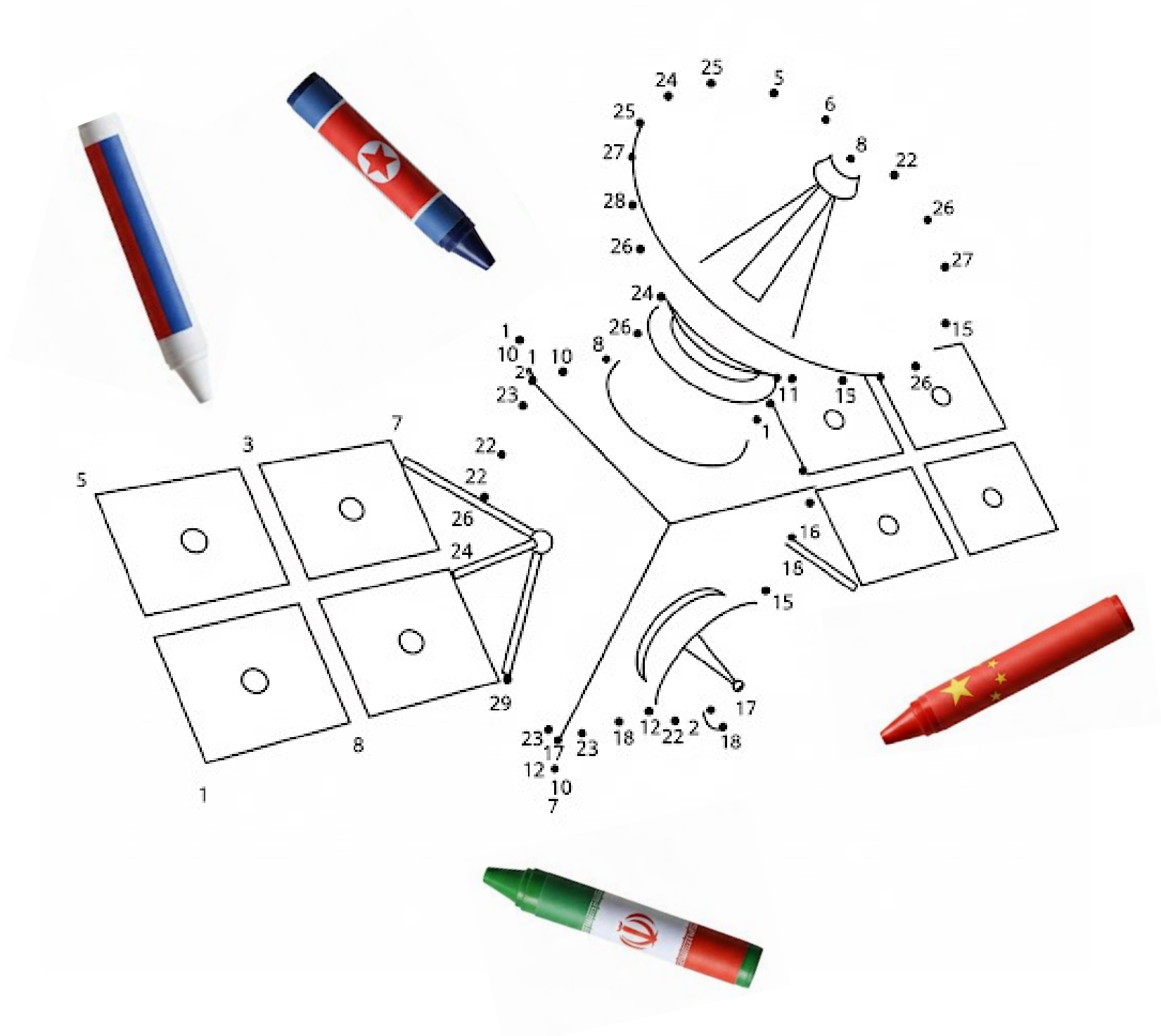


[Protect and store sensitive information properly.]

[Comply with SEAD 3.]



LET'S SECURE THE DOTS



BEFORE THEY CONNECT THE DOTS

SUPPLY CHAIN SECURITY...

PERIOD!



Secure the Dots!

SECURING

CLASSIFIED ENVIRONMENTS



▪ TRUSTED GUARDS • SURVEILLANCE SYSTEMS • ACCESS CONTROLS • INFOSEC PROTOCOLS ▪

Securing Classified

Get smart about

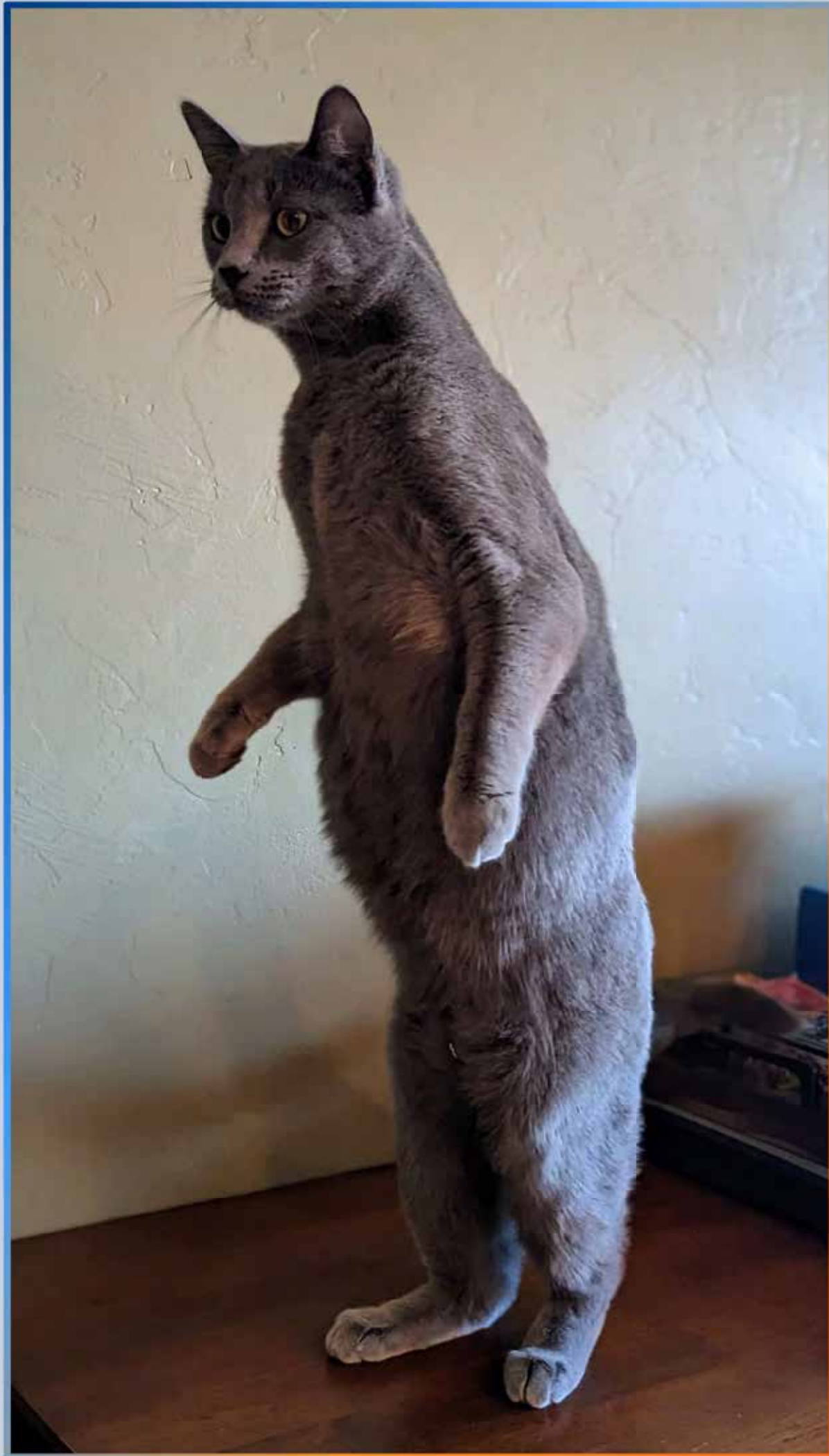
SECURITY!

*Everything you need to know
rolled up in one package.*



Security Smarts

THINGS AREN'T ALWAYS AS THEY SEEM...



**SEE SOMETHING
SAY SOMETHING**



See Something Say Something

LET ME TELL YOU A SECRET!



Verify Need to Know and Clearance Levels before disclosing any classified information.

Never trust anyone with sensitive or classified information, no matter how cute they are!

Small Puppy Secrets

Stars, Stripes, and Security



*PROTECT THE INFORMATION
THAT PROTECTS OUR NATION.*

THINK BEFORE YOU SHARE.

Stars and Stripes

Reportable Suspicious Contact

Foreign Intelligence Entities (FIE) commonly use a method and technique called **elicitation** to collect intelligence through what appears as normal, even mundane, social, or professional contact.

An FIE method of operation attempts to confirm or expand their knowledge of a sensitive program or gain clearer insight into a person's placement and access (P&A) prior to possible recruitment.



Don't Be Fooled!

**Code of Federal
Regulation (CFR) 32
Part 117
National Industrial
Security Program
Operating Manual
(NISPOM)**

**Requires the reporting of
suspicious contact,
behaviors, and activities.**

Get to know your FSO!



Suspicious Contact

Suspicious Kittens

187

Don't sweep it under the rug
Report to you FSO
in a timely manner



Let's clean it up right the first time around

Sweep It Up_SEAD3

Team Effort

THINK BEFORE YOU CLICK!

STOP PHISHING SCAMS

Don't take the bait!



SECURE YOUR PASSWORDS

Use Strong & Unique Passwords



USB SAFETY

Think Before You Plug In!



BEWARE OF SOCIAL ENGINEERING

Don't Trust Strangers!



PROTECT YOUR DATA. STAY VIGILANT!

REPORT ANY SUSPICIOUS ACTIVITY IMMEDIATELY!

Think before you click



REMEMBER TO COMPLETE YOUR ACTIVITY
SECURITY CHECKLIST WHEN LEAVING
FOR THE DAY

Transguide

SECURITY ISN'T JUST WHAT YOU LOOK AT...

IT'S WHAT YOU NOTICE.

INATTENTIONAL BLINDNESS IS WHEN YOU **MISS OBVIOUS RISKS** RIGHT IN FRONT OF YOU.

WHAT CAN YOU MISS?

-  **TAILGATING**
-  **SUSPICIOUS BEHAVIOR**
-  **UNAUTHORIZED DEVICES**
-  **SENSITIVE INFO REQUESTS**
-  **CHANGES IN COWORKER BEHAVIOR**

THE SECURITY PROFESSIONAL'S RULE:

-  **PAUSE.**
-  **OBSERVE.**
-  **QUESTION.**
-  **REPORT.**

EVERY EMPLOYEE IS PART OF SECURITY!



PROTECT THE MISSION.



PROTECT YOUR COWORKERS.



PROTECT NATIONAL SECURITY.

WHEN IN DOUBT—

REPORT IT!

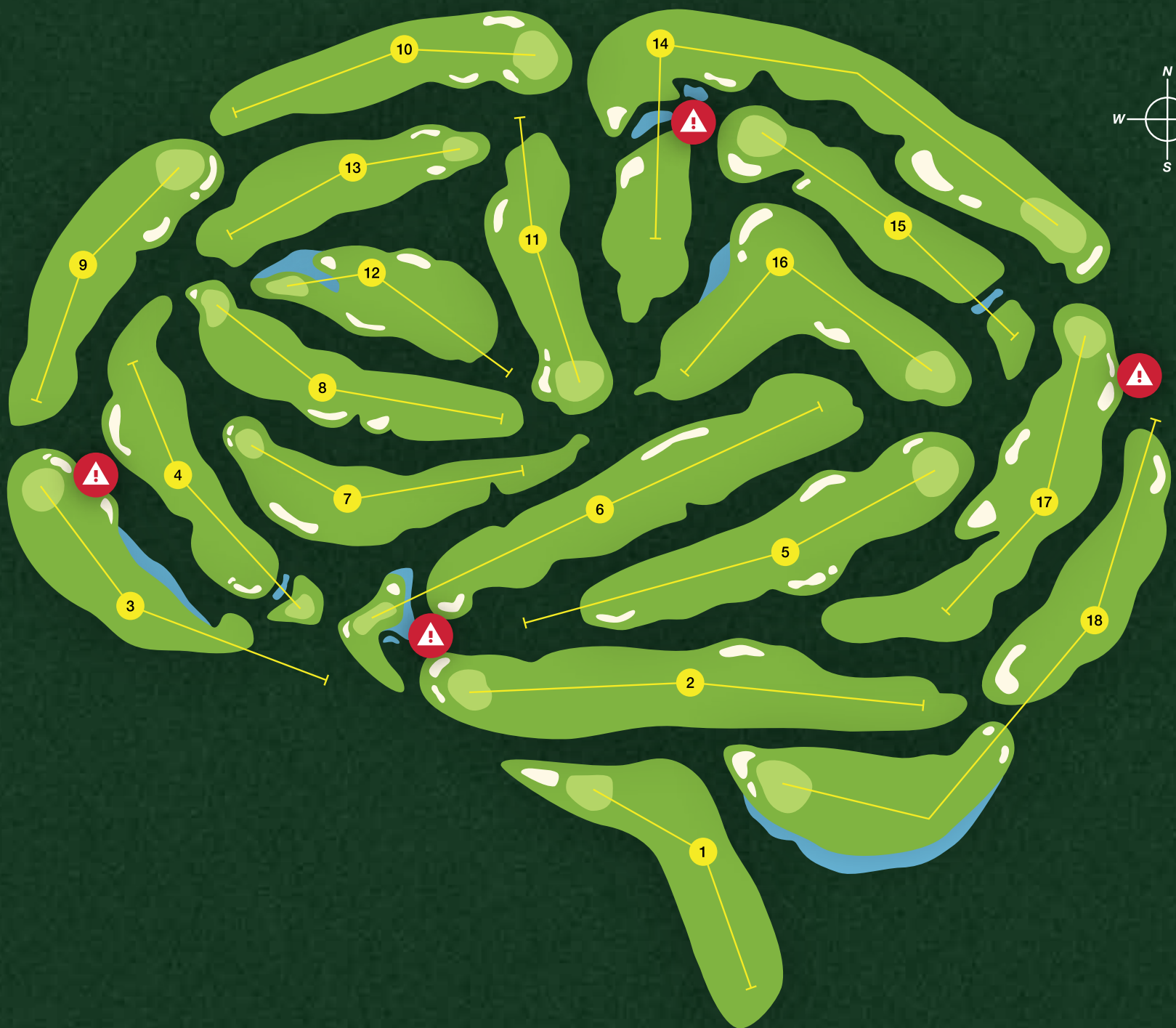
IT'S **NEVER** WRONG TO REPORT IN GOOD FAITH.



What you notice

BECOME
MASTERS
OF
BEST PRACTICES

STAY ON PAR WITH GOOD SECURITY



HAZARDS TO KEEP TOP OF MIND

- ⚠ Weak Passwords
- ⚠ Public Wi-Fi
- ⚠ Unlocked devices and information
- ⚠ Untrusted email links and attachments



Masters Best Practice



*Good security practices
are peachy keen!*

CDSE 

Peachy Keen

Bad Security Practice is the **Pits!**



KEEP SECURITY ON YOUR MIND

Center for Development
of Security Excellence

CDSE



Pits

195

Be a Peach,
Don't Spill the Tea



Prevent Spillage
Safeguard Information & Activities



Prevent Spillage

SECURITY

*** Protecting America's ***

WARFIGHTERS



THEN. NOW. TOMORROW.

*** 1776-2026 ***



CDSE



NCMS

250 Years & Counting

Warfighters