DEPARTMENT OF THE ARMY
Office of the Deputy Chief of Staff, G-3/5/7
400 Army Pentagon
Washington, DC 20310-0400

DAMO–ZCA

Mr. William Marshall
425 Third Street, SW Suite 800
Washington, DC 20024

30 NOV 2016

Dear Mr. Marshall:

This letter responds to your August 22, 2016 Freedom of Information Act (FOIA) requesting the entire PowerPoint presentation on operational security delivered to Soldiers at Fort Leonard Wood that contained a slide depicting Gen. David Petraeus and former Secretary of State Hillary Clinton, among others, as examples of "insider threats." Your request was processed in accordance with Title 5 United States Code Section 552, The Freedom of Information Act.

The briefing presentation is partially releasable (enclosed) in accordance with FOIA Exemption 6 (5 U.S.C. Section 552(b) (6)). Exemption 6 permits us to withhold personally identifying information, the release of which would substantially compromise individual privacy interests. Personally Identifiable Information for the military and civilian personnel listed in the document is being withheld.

My withholding of this information constitutes a partial denial of your request. You may appeal this decision within sixty days of the date of this letter through this office, HQDA, DCS G-3/5/7, Attention: FOIA Office, 400 Army Pentagon, Washington, DC 20310-0400, to the Secretary of the Army, Attention: Office of the General Counsel, Washington, DC 20310-0104. There are no assessable fees for your request.

If you have any questions regarding this response, please contact the G-3/5/7 FOIA Officer at (571) 256-7607 or usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.foia@mail.mil

Sincerely,

Kurt W. Fedors

Encl

KURT W. FEDORS
Administration and Resources Directorate

Correct Spelling?

A – idiosyncrasy

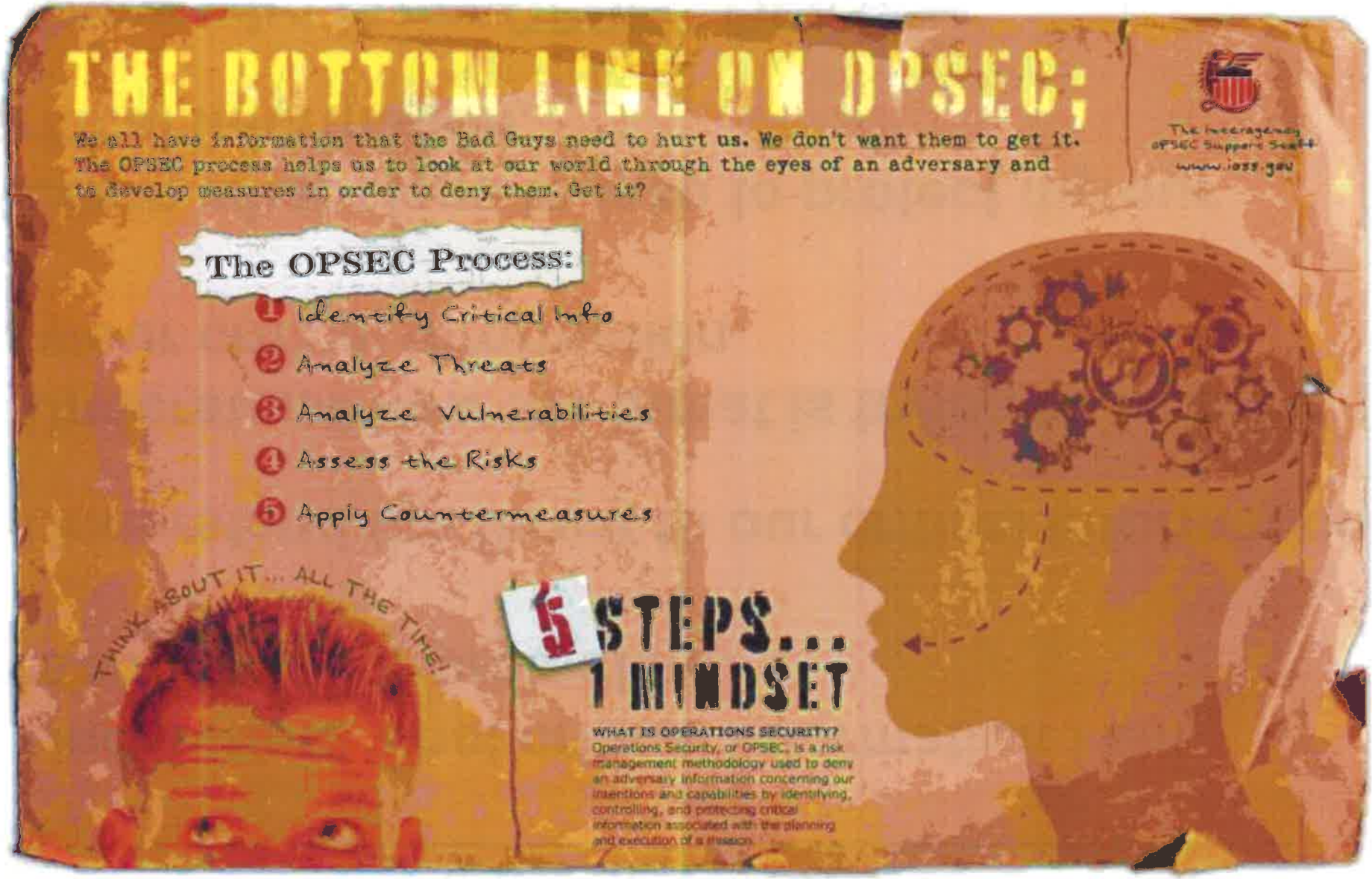
B – idiosincracy

C – ideosyncrasy

Riddle Me This?

- I am the beginning of everything, the end of time and space, the beginning of every end, and the end of every place. What am I?

Army
Annual OPSEC Level I Training 2016



Objectives today

- Understand what critical information I am responsible for protecting.
- Understand the threat to our critical information.
- Understand how the threat is trying to acquire my/our critical information.
- Learn what steps to take to protect my/our critical information.
- Know who is my OPSEC Officer.

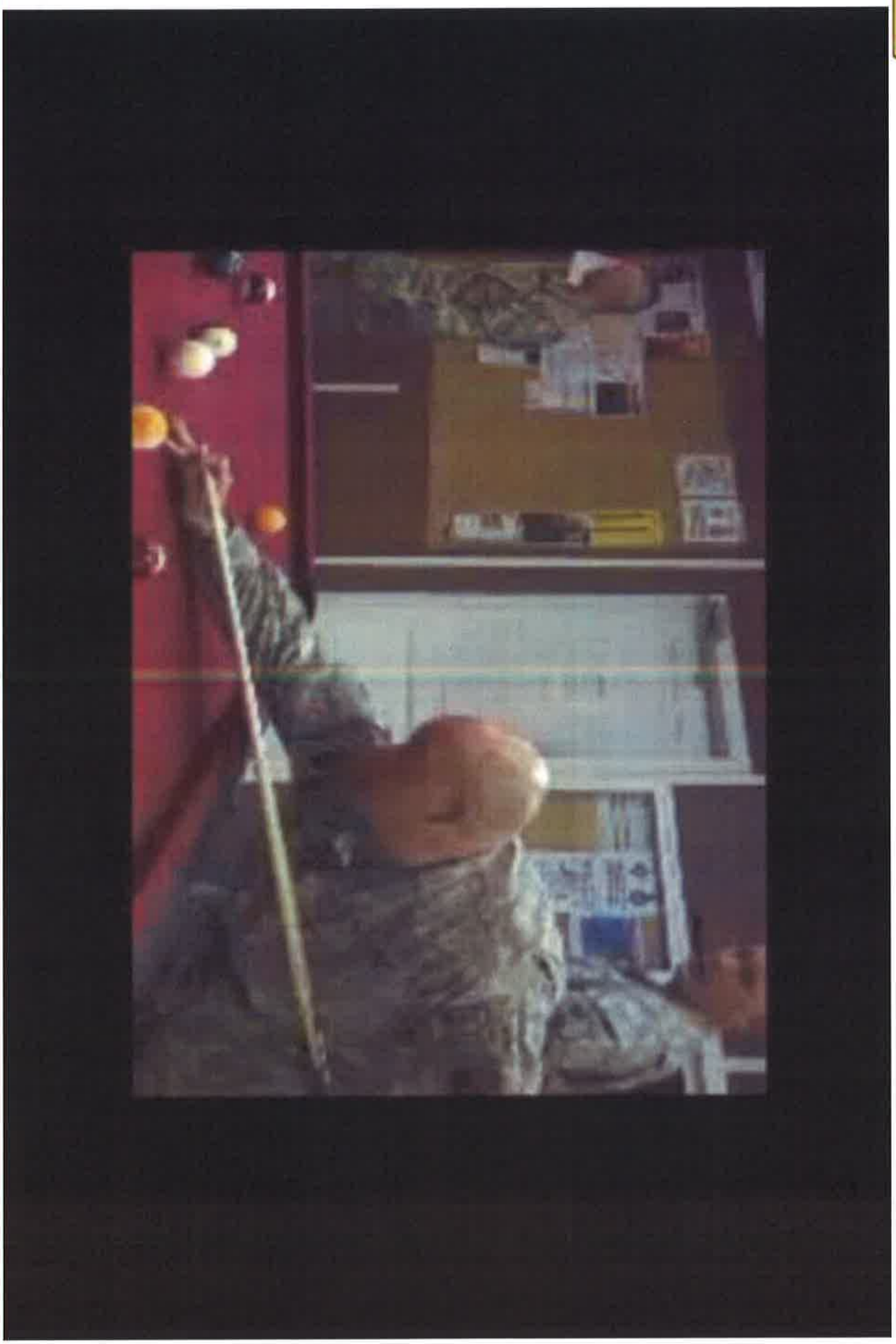
OPSEC is not New

References

"The general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack"

Sun Tzu, 200 B.C.

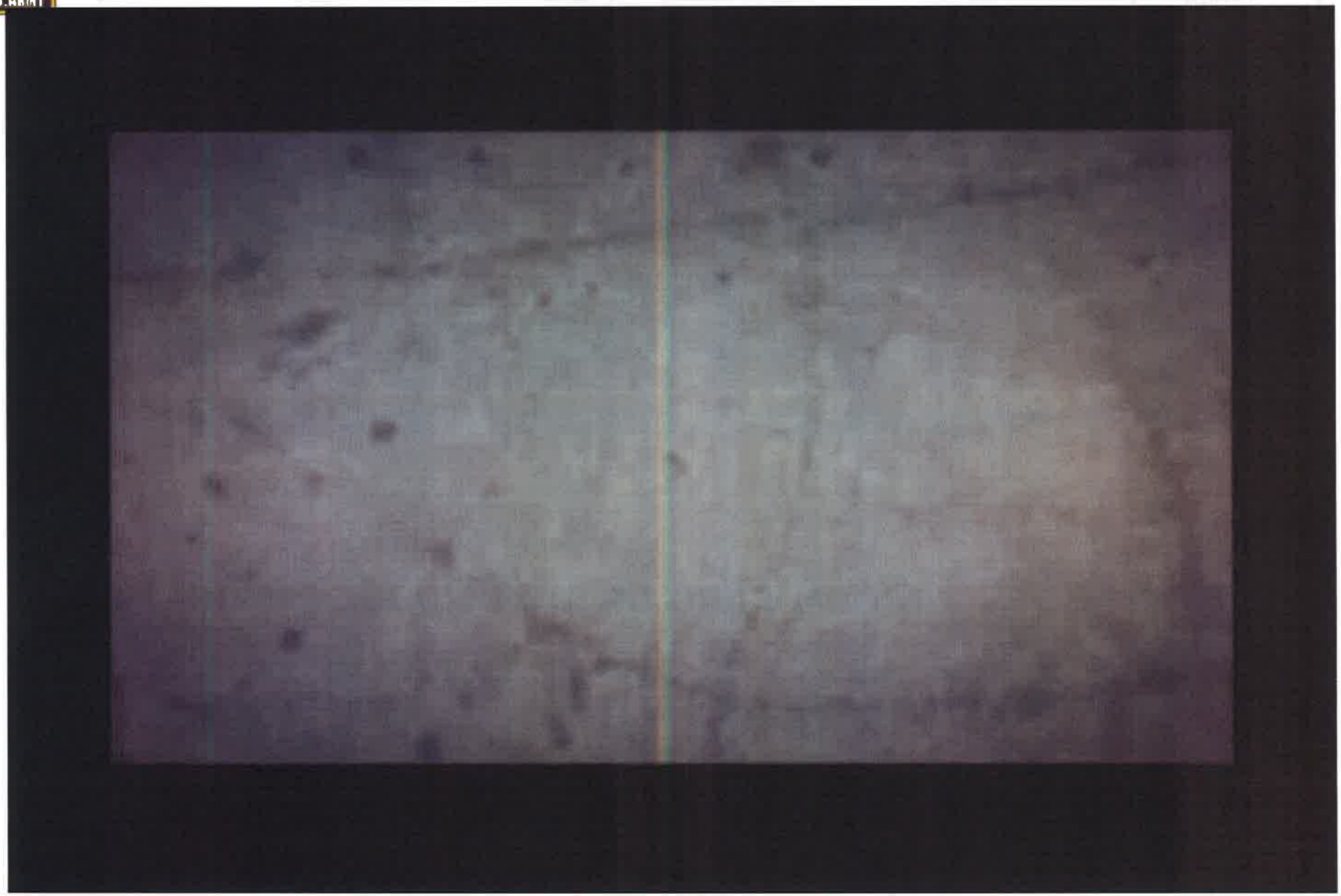
- National Security Decision Directive 298
- DoD Directive (DoDD) 5205.02 E
- AR 530-1, Operations Security, 26 Sep 14.
- TRADOC OPSEC Plan 14-013, 30 Jul 14.
- MSCoE OPSEC Plan 15-002



What is OPSEC?

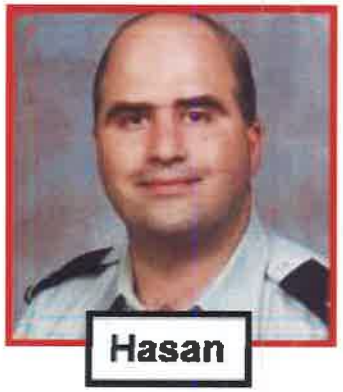
- "**Operations Security**".
- It is **not a traditional security program** such as Physical Security, Information Assurance, or INFOSEC, **it is a mindset** that all of us must develop to protect our mission, personnel, and resources.
- OPSEC is used to **deny our adversaries UNCLASSIFIED CRITICAL and SENSITIVE** information about our organization's Capabilities, Activities, Limitations and Intentions (**CALI**), that can be used against our organization.
- Critical or sensitive information includes **For Official Use Only** (FOUO) (information protected by the Freedom of Information Act), our **Critical Information List (CIL), Personally Identifiable Information (PII),** as well as information covered by the **Health Insurance Portability and Accountability Act (HIPAA).**

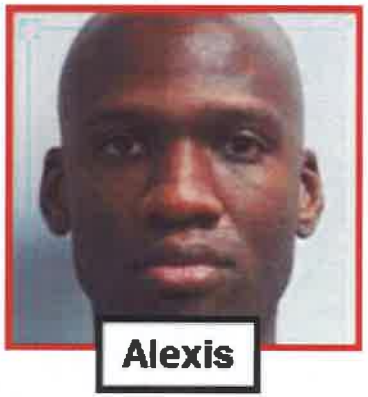
Who is the Threat?



Who is the Threat? Insiders

- Insiders
  - Hasan, Manning, Snowden, Alexis
  - Careless or disgruntled employees

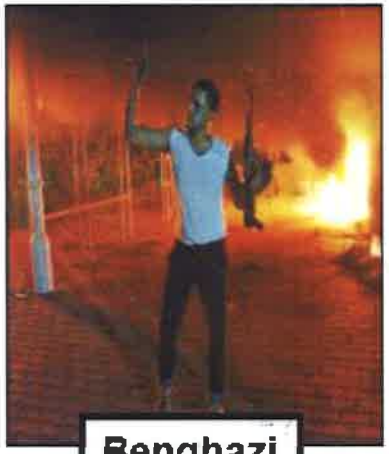


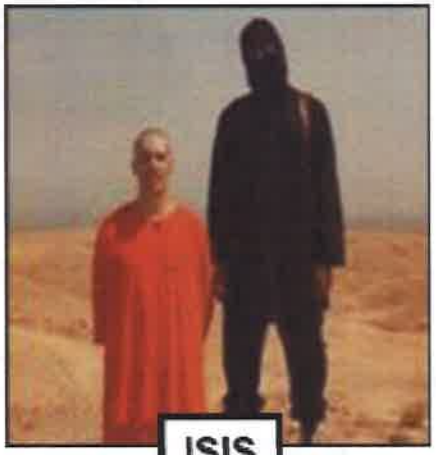


Who is the Threat? HVE &Terrorist

- Terrorists - Domestic and International


Boston

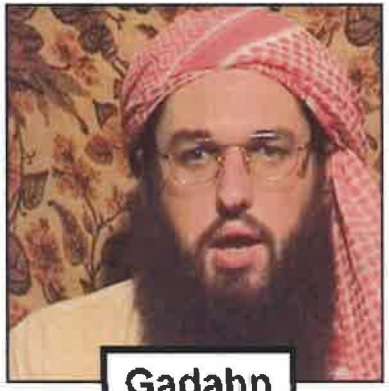

Benghazi

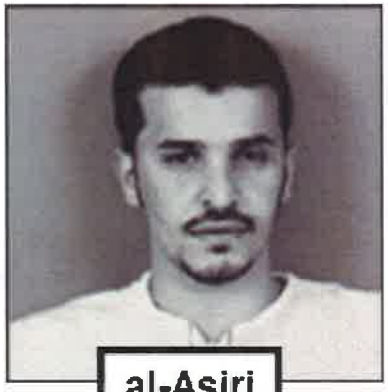

ISIS


Paris


Tsarnaev


Muhammad/Bledsoe


Gadahn


al-Asiri

Who is the Threat? Foreign Govs & Criminals

- Foreign Governments – FIS & Allied Nations

- Criminals - Hackers, Scam Artists, Identity Thieves, Property Thieves, OMGs/1%ers

What do they want?

- Our Capabilities, Activities, Limitations, and Intentions (CALI).

- Specific operations plans, TTPs, future force structure, unit readiness.
  - Who, what, when, where and how we operate or will in the future. *Would MU give this type of info to KU before the game? Do we give this to our adversaries in our emails, blogs, social media, trash, etc?*

- Our security processes.
  - Where are we vulnerable? When? How?

HOW ARE YOUR SECURITY MEASURES WORKING?

Victory Starts Here!

U.S. ARMY

MSCoE Critical Information List (CIL)

Updated annually – approved by CG; Found on FLW Homepage – Common Operational Picture (COP)

a. Vulnerabilities and security measures of MSCoE's communication and information systems, both current and new technologies.

b. Sensitive, non-public major MSCoE events, times, locations, attendees, and security plans.

c. Itineraries of general officers (GOs), senior executive service (SES), very important persons (VIPs), and distinguished visitors (DVs).

MSCoE Critical Information List (CIL)

d. Vulnerabilities that affect FLW in relation to access, disasters, and infrastructure; and protective measures employed to protect them.

e. Results of assessments, surveys, data analysis, and performance measures for FLW operations and programs that may reveal capabilities and vulnerabilities.

f. Plans for initiation of contingency operations, and deployment/re-deployment or mobilization/de-mobilization of units affecting FLW.

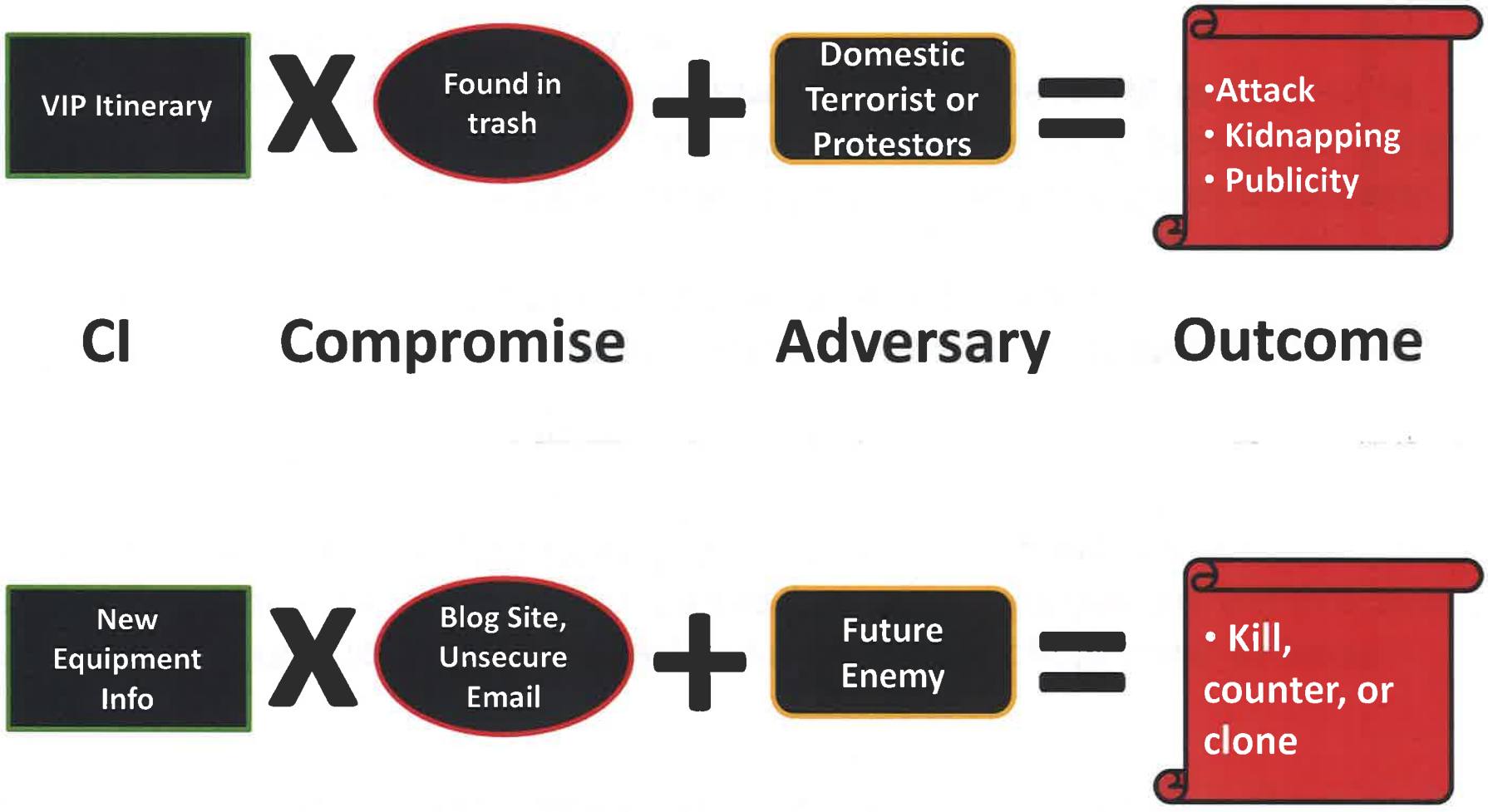
MSCoE Critical Information List (CIL)

g. Protection and response capabilities of FLW assets, activities, or service providers on or off the installation.

h. Training status, available inventory, and capabilities of FLW units, to include K-9 operations.

i. Serious morale problems that exist within FLW.

Critical Information Compromises



How do they get our information?

- **Social Engineering:** Phone calls, emails, requests for information about you or your organization. Is that really your bank or another unit asking for that data?

- **Surveillance:** What is on/in your car, in your trash/recycle bins, in your unencrypted emails, on the security badge you wear outside the secure area? What do you leave out on your desk? What discussions are you having "in the open"?

- **Cyber:**
  - Phishing - Socially-engineered e-mails containing infected attachments and/or hyperlinks that lead to web sites hosting malware.

  - Using unauthorized Commercial Mobile Devices for official purposes. Hackers are rapidly developing malicious applications & programs for the new tablets, smartphones, & e-readers. Very little security is built-in or readily available on these devices.

- **Web:** What are you, your family, or your fellow employees posting, texting, and placing on social media? Can it be used to social engineer you?

Open Source

Up to 90% of adversary's intelligence needs can be satisfied, mostly risk and cost free.

Media | Library | Internet | Newspapers | Magazines | Trade Publications | Public Records | Congressional Hearings | Weblogs | Contract Specifications | Social Media | Academia | Freedom of Information Act Requests | Courseware | Budget | Digital Databases | Reports | Nongovernmental Organizations (NGOs) | Conference | Lectures | Rally | Unsecure Cloud | Book | Radio | Newsgroup | Chat | Webcast | Webcam | Directory | Geospatial | Global Security.Org | Maps | Manuals | Direct Observation | Blueprints | Building Plans | Search Algorithms | Schedules | Discarded Electronics or Disks

Trends

- **Lack of OPSEC Reviews.** HQDA and local policies require that all documents must receive an OPSEC review before being released or posted to the public domain. Includes contracts and unit web/social media pages.

- **PII loss.** PII is often found in the trash, on people's social media sites. Where do you have your DOB posted? Your mother's maiden name? *(password reset answers)*. When emailing, use encryption.

- **Computer Use.** Using personal Emails/Web Links, or personal mobile devices for Official Business, particularly when it comes to CIL or FOUO.

- **Badges in public.** Badges can be cloned, hide or remove them when you leave the secure area. The parking lot is not a secure area.

- **Trash INT.** Take a look in the trash cans and recycle bins in your areas. Many FOUO, PII, and CIL information can be found there. Adversaries know this.

- **Unauthorized cell phones in Secret briefings/VTCs.** What about new smart watches?

- **Social Media.** Web Postings are subject to surveillance and personnel can be held to administrative action for their unauthorized postings.

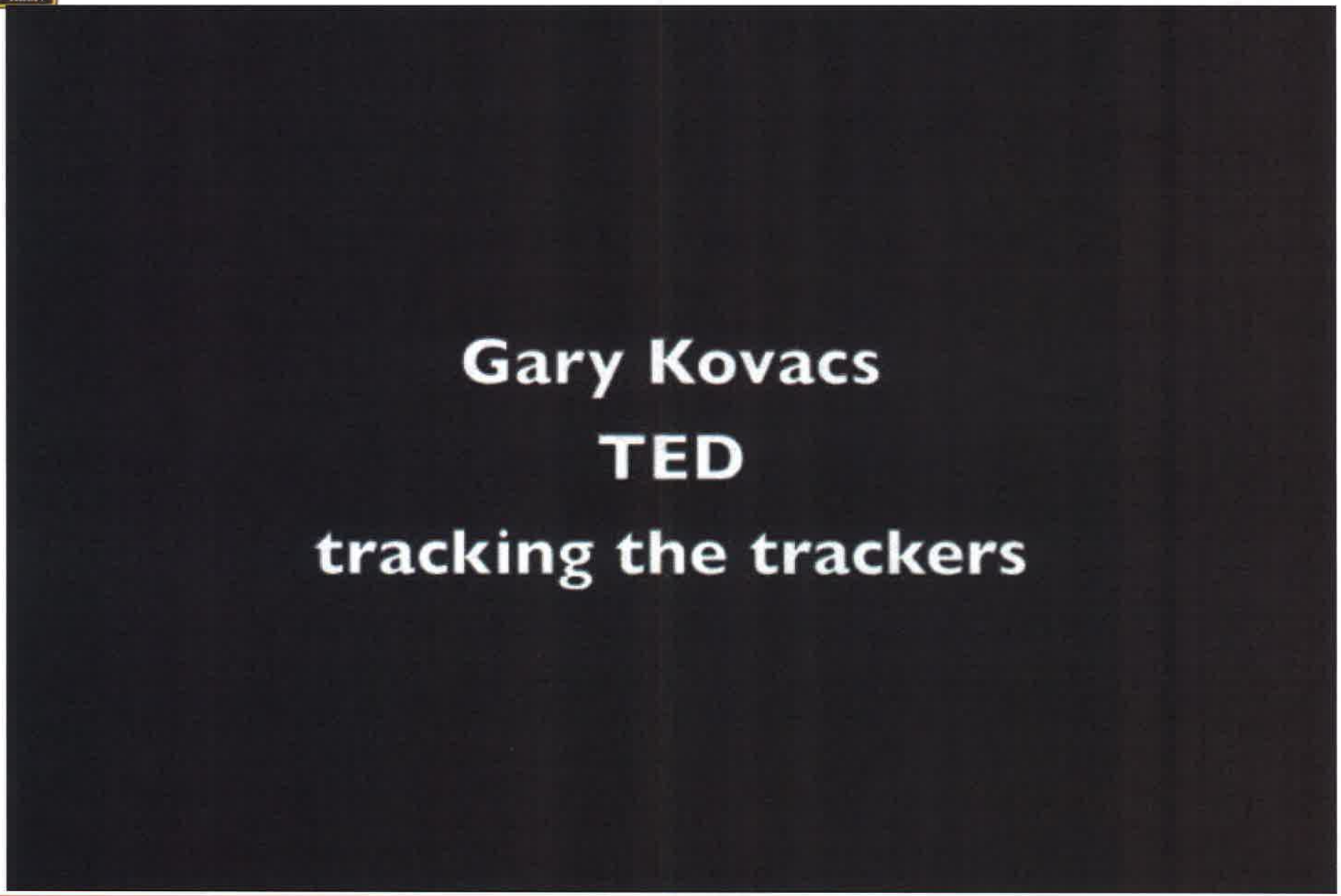
In Cyberspace, where is your information going?

Tens of thousands of new malicious software programs or variations are identified every day

The frequency and sophistication of intrusions into U.S. military networks have increased exponentially in the past 10 years

Military networks are probed thousands of times and scanned millions of times every day

Dangers of Cyberspace



How can you help stop them?

- **Consider the threat when you:**

- Go on-line, use the phone, text, or email
- Discuss work in public places, or answer a stranger's questions
- Dispose of documents

Shred it or regret it!

OPSEC Measures

- Critical or sensitive information must be encrypted when disseminated via e-mail within Army information systems.
- Ensure that government conversations, web postings, blogs, social media comments, or releases to the media and/or public receive appropriate OPSEC reviews prior to release.
- Do not wear security badge(s) outside secure areas. Avoid allowing pictures to be taken of security badge(s) and/or other sensitive information in the background.
- Briefings: Ensure that notes taken are properly marked, handled, collected, or maintained by authorized personnel and/or destroyed afterwards.

OPSEC Measures

- Do not use public or personal computers for Government business.
- Social Media: Do not reveal sensitive information about yourself such as mission schedules, briefings, and event locations. Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of me, my family or my unit?". Inform family members.
- Log off computer or remove CAC when away from work area.
- Limit use of personally owned devices, to include mobile devices, to only those documents that are approved for public release. Do not download FOUO or other distribution restricted documents and files to your personally owned devices. This includes emailing the documents to a personal commercial email.

Do Family Members know Critical Information?

FLW OPSEC Officers

- MSCoE (b) (6) (b) (6)
- MSCoE (b) (6) (b) (6)
- Gar Cmd (b) (6) (b) (6)
- 1st EN Bde (b) (6) (b) (6)
- USAES (b) (6) (b) (6)
- 3rd CM Bde (b) (6) (b) (6)
- USACBRNS (b) (6) (b) (6)
- 14th MP Bde (b) (6) (b) (6)
- USAMPS (b) (6) (b) (6)
- 43rd AG Bn (b) (6) (b) (6)

Check on Learning

- Understand what critical information I am responsible for protecting.
- Understand the threat to our critical information.
- Understand how the threat is trying to acquire my/our critical information.
- Learn what steps to take to protect my/our critical information.
- Know who is my OPSEC officer.

Other Resources

- **Army OPSEC Facebook page at** https://www.facebook.com/#!/pages/Army-Operations-Security-OPSEC/163005357133404?fref=ts
- **IOSS web site at** https://www.iad.gov/ioss/
- **OPSEC For EOP Operators (Social Media) at** https://iatraining.us.army.mil
- **NetSmartz at** http://www.netsmartz.org/Parents

THE END