Civil Air Patrol

OPSEC Briefing

LtCol Ed Wolff, CAP/DOKS

OPSEC- What is it?

"**Operations Security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified - concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other**

security disciplines –

it supplements them."
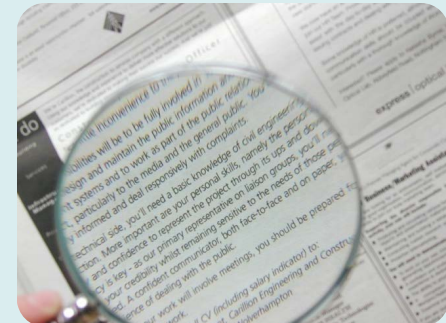
In other words…

OPSEC helps you control information that could be used against you.

OPSEC can be used to increase safety and security in ANY setting and for ANY purpose.

Why OPSEC?

- **Why does CAP need OPSEC,**

  …..“we are just the CAP”…
  - **New emerging missions**
    - **Communications**
    - **Operations**
  - **Part of the “Total Force”**
    - **AFI 10-701 OPSEC**
  - **Keep people safe**
  - **Keep the program operational**
  - **Accomplish the Mission!**

UNCLASSIFIED

OPSEC is:

- **A process that helps you examine your day-to-day activities from an adversary's point of view**

- **A tool that helps you understand what an adversary can learn about your organization from your activities.**

- **A risk assessment tool**

OPSEC is:

- **A way to identify security risks and countermeasures**

- **A method that can be adapted to any operation, program, event or situation**

- **A cost-effective addition to your security arsenal**

- **A mindset, a way of life!**

OPSEC is not:

- **A strict set of "rules" and "procedures"**
- **An expensive and time-consuming process- OPSEC can be low-cost or free**

OPSEC

No matter your position, rank or function, YOU have a part to play in OPSEC. Pilots, observers, communicators, incident commanders, admin staff, squadron-group-wing commanders, etc. All one team with one mission.
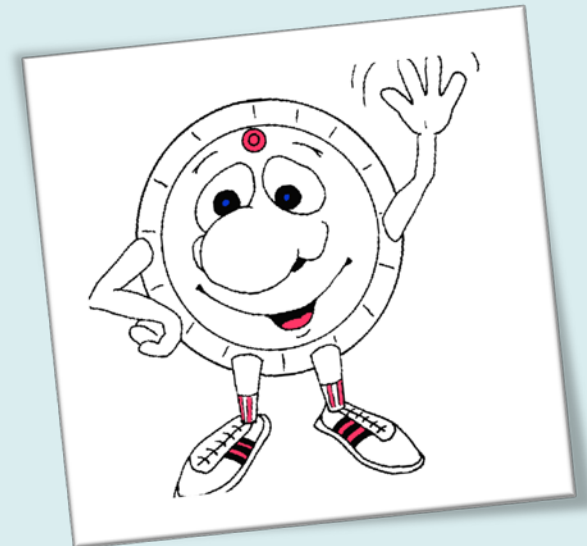
Every Person Is
An OPSEC Sensor!

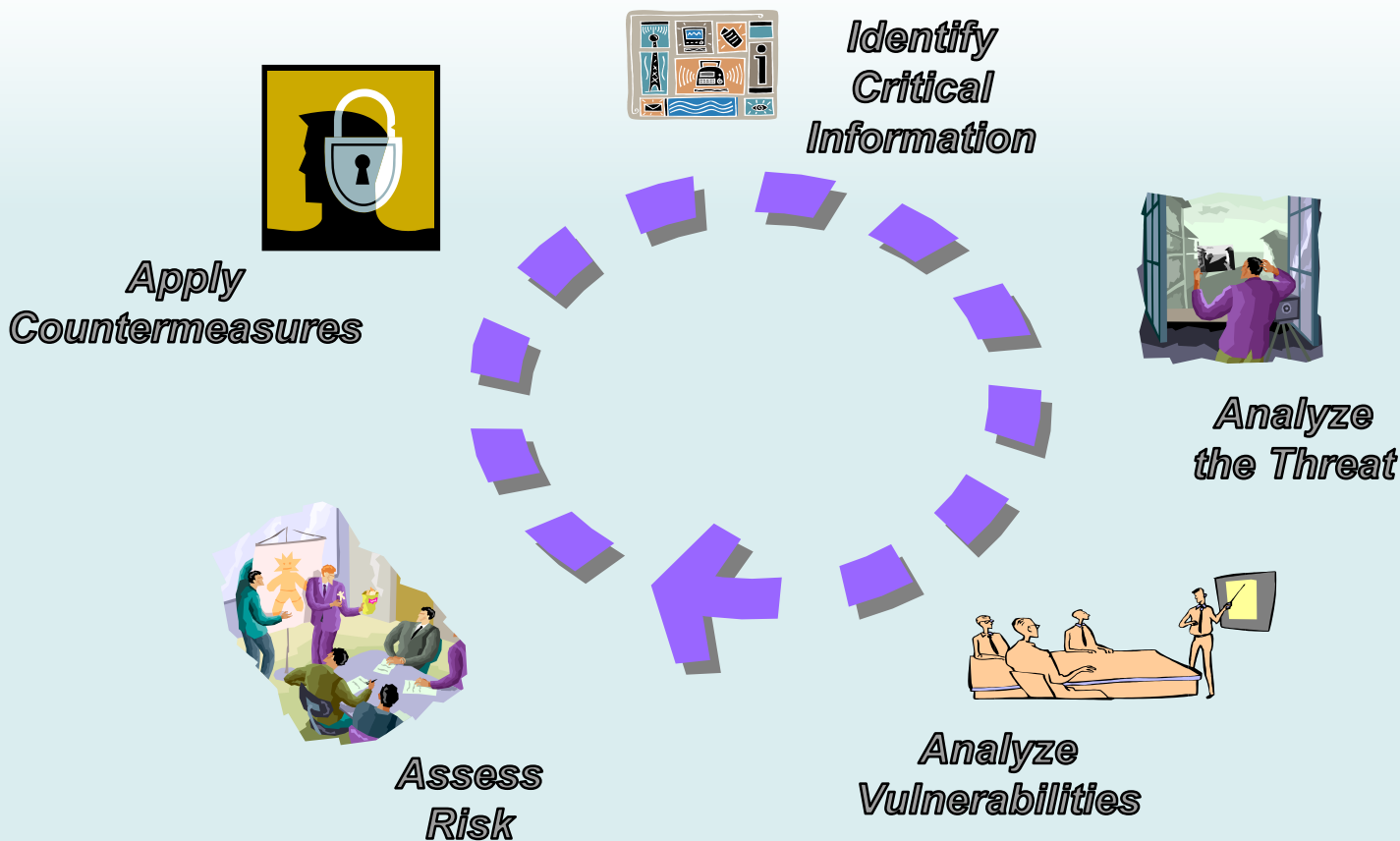Every person in the CAP is able to be a part of the security solution by:

- ✓ **Knowing the threats**
- ✓ **Knowing what to protect**
- ✓ **Knowing how to protect it!**

UNCLASSIFIED

The OPSEC "5-step Process"

Identify Critical Information

Analyze the Threat

Analyze Vulnerabilities

Assess Risk

Apply Countermeasures

UNCLASSIFIED

Definition:
"Risk" and "Impact"

"Risk" is the probability that an adversary will compromise your critical information.

"Impact" is the effect that this compromise would have on your organization. Impact is the "what would it mean" factor.

The enemy is watching…

In this digital world, there are very few truly "primitive" enemies. The enemy is:

Watching Chatrooms

Following Tweets

Sending social engineering email ("phishing")
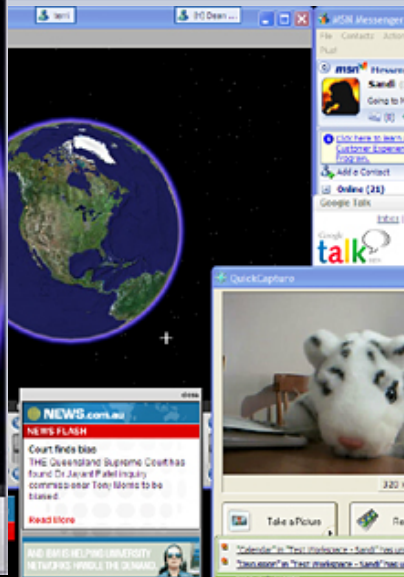

Monitoring Forums

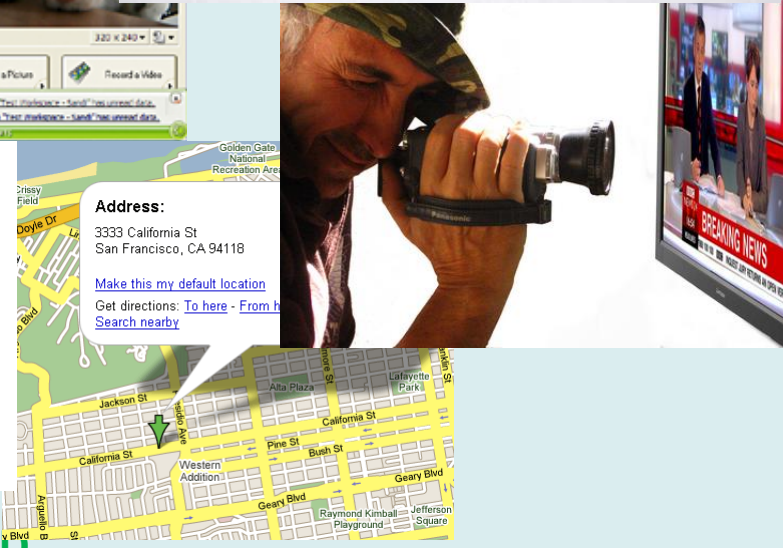Connecting on Social Media

Listening

UNCLASSIFIED

And they have the same that our forces use:

peopledetectivesearch.ws

Search Who: [   ]   Where: [All 50 States ▼]

Enter the code shown: *8v8a* [   ]   [Search]

Consider your footprint…

- **Where would you find information about your missions?**

- **Have you issued press releases?**

- **Do your members have personal blogs?**

- **Is there information in Google News?**

- **Is there a regular newsletter that's publically available?**

- **Everywhere that information exists about the missions of the CAP can be a possible piece of the puzzle.**

UNCLASSIFIED

A note on public websites:

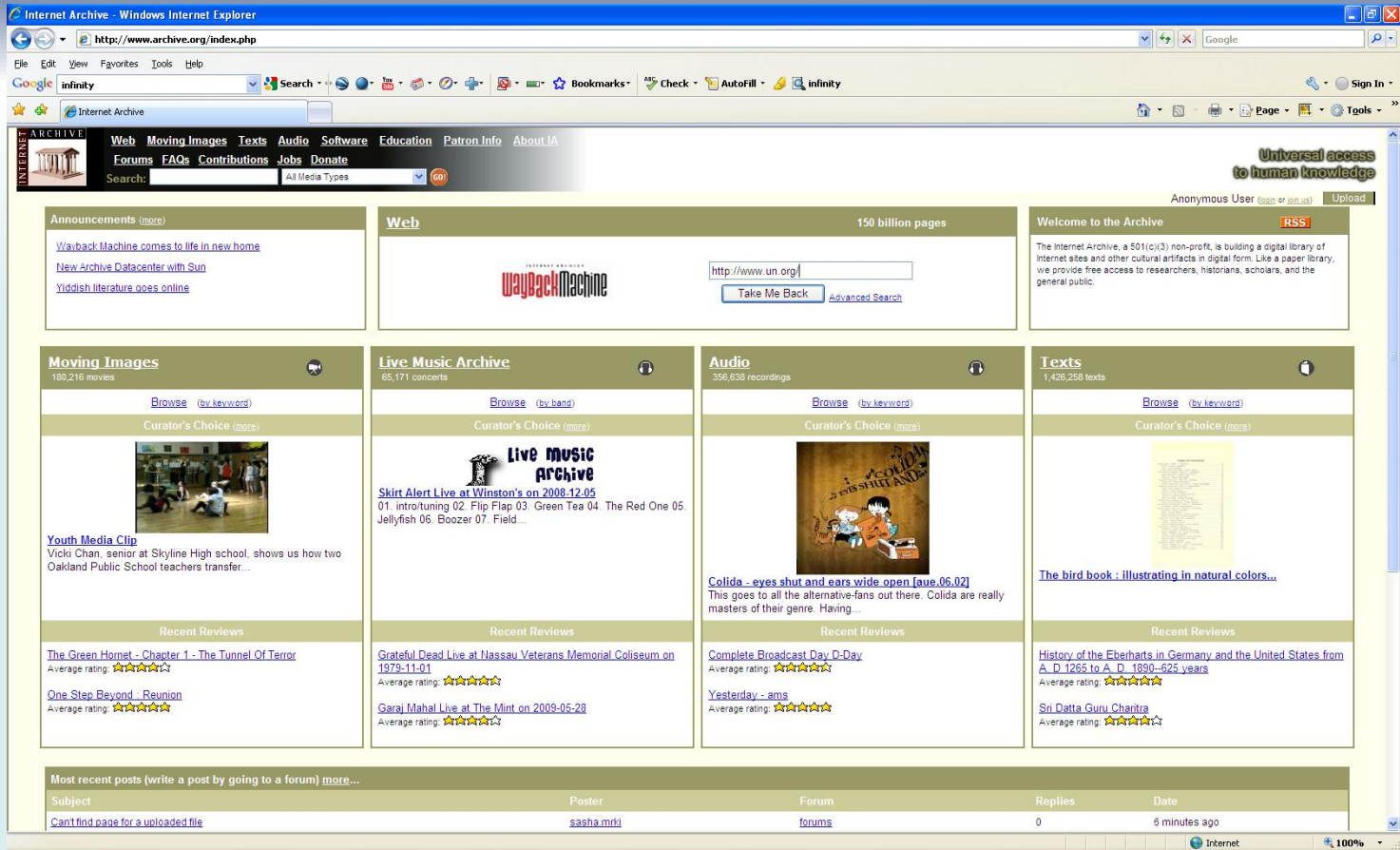Certain things should not be found on public websites, blogs, etc., including:

- **Sensitive Operations Plans**
- **Sensitive Communications Plans**
- **Alerting Lists, With Names**
- **By Name Personnel Lists**
- **Locations of Sensitive Assets (Vehicles, Airplanes, Radios, etc)**
- **Locations of Sensitive Facilities (EOC's, COOP Sites, etc)**

UNCLASSIFIED

For Example:

The "Internet Wayback Machine" takes periodic "snapshots" of website content.
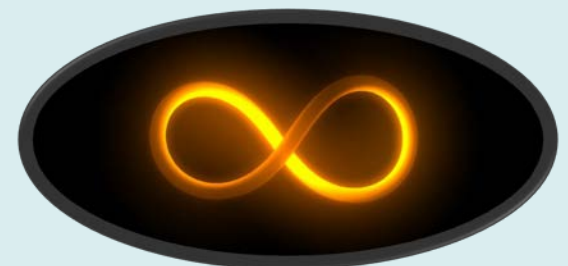
"It" never goes away!

When you put information on the net, via your blog, Facebook, Instagram, email, etc., you have to assume that it's going to stay there forever.

Same thing with newspapers, magazines, and other media.

The only safe bet is to make sure that it never gets there in the first place!

UNCLASSIFIED

REMEMBER

It is the responsibility of the security professional to answer those questions for the end-users

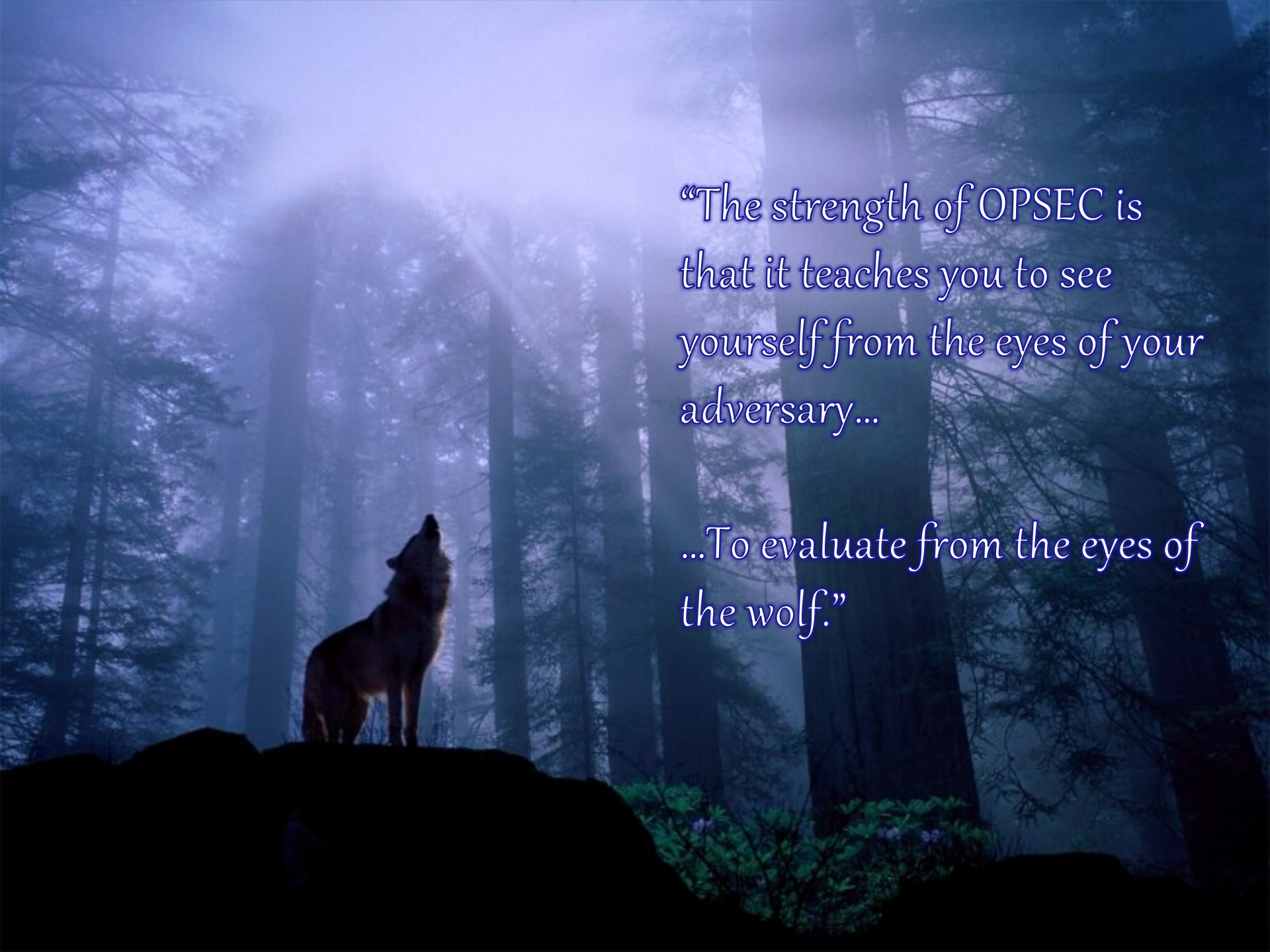It is the responsibility of the end-users to do it!

Conclusion

OPSEC is what you make of it

- **The way ahead**
  - **Annual OPSEC training requirements in compliance with AFI 10-701**
  - **OPSEC Survey**
  - **OPSEC evaluations of CAP web sites (already started from the DOK side)**
  - **OPSEC awareness emphasis at the Squadron, Group, Wing, Region and National levels.**
  - **New emerging missions will drive this requirements for enhanced OPSEC awareness**

"The strength of OPSEC is that it teaches you to see yourself from the eyes of your adversary...

...To evaluate from the eyes of the wolf."

Civil Air Patrol

CITIZENS SERVING COMMUNITIES
UNCLASSIFIED