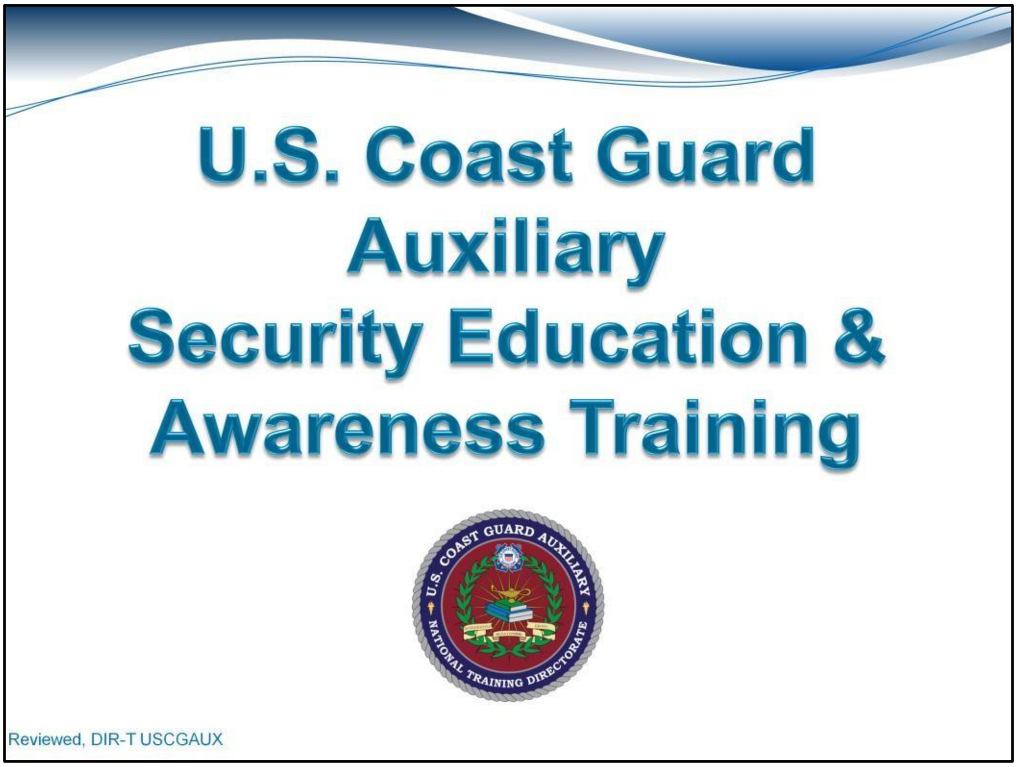


U.S. Coast Guard Auxiliary Security Education & Awareness Training

Reviewed, DIR-T USCGAUX

. Welcome to the US Coast Guard Auxiliary **Security Education & Awareness** Training.

Independent Learner Instructions.

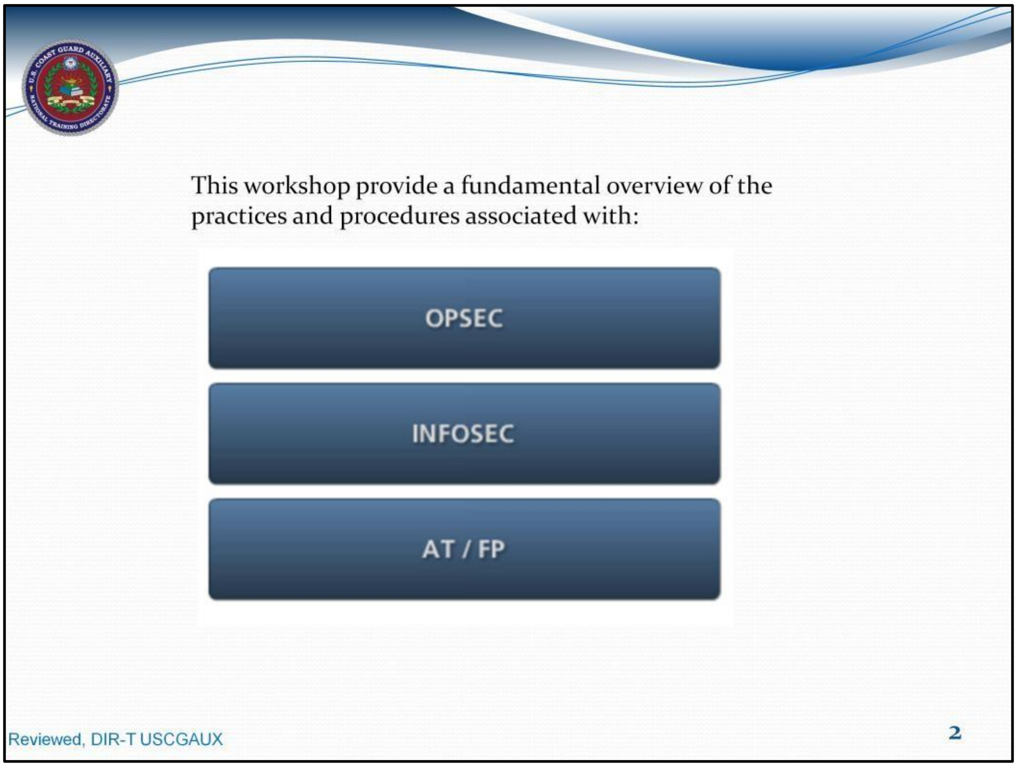
This document is derived from the mandatory training of the same name. It contains both images and narratives regarding the training topic and is provided in a “presenter notes” format.

As an independent learner you are expected to read all content contained in this document to include both the text within the images and the notes below the image (if any). Some images do not have notes or are self-explanatory.

As you work through this training material you should keep in mind that as an independent learner, you are responsible and accountable for learning and understanding the course content.

You should also understand its importance to our organization and the execution of our varied missions and be able to apply the knowledge gained through this independent training experience.

As a member of the coast guard workforce you have a responsibility to help maintain awareness protect information and act to prevent threats. Recognizing the signs of a potential terrorist acts or security breaches will help to prevent acts on the homeland and activate appropriate response units.



This workshop provide a fundamental overview of the practices and procedures associated with:

- OPSEC
- INFOSEC
- AT / FP

Reviewed, DIR-T USCGAUX

2

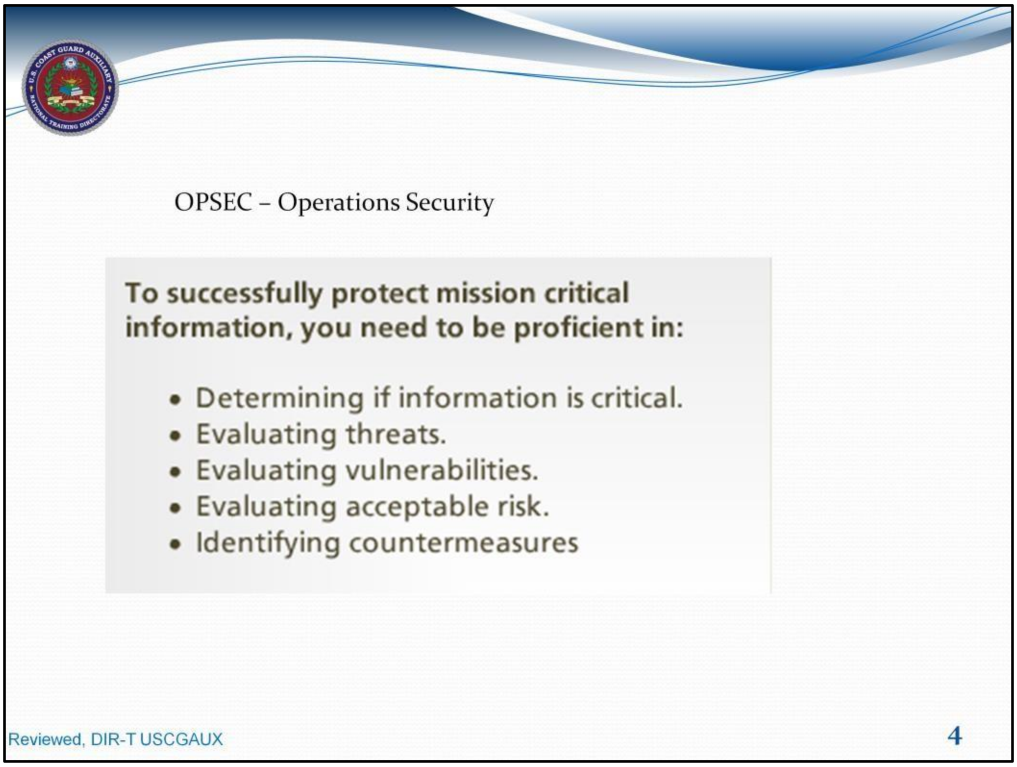
When you recognize the potential threat you have the power to stop it before it can cause harm to the Coast Guard and its missions which of the following do you think is true of our enemies? Most acts are the result of years of coordinated research and surveillance that provide sensitive information to the enemy. Bits of information, both classified and unclassified, can be put together to provide a detailed picture of the adversary of our vulnerabilities and operations. It is your responsibility to be aware of your surroundings and report any activity that could jeopardize the Coast Guard’s mission, even if it involves someone you know or work with.

Throughout your career you will be entrusted with information critical to Coast Guard missions. You must protect this information to safeguard both missions and people. Be cognizant of this responsibility and do not take it lightly. This module provides review of security fundamentals. In each of the three lessons you'll have the opportunity to demonstrate the decision skills necessary to safeguard information. protect the mission your shipmates and yourself, you'll need to complete each of the three lessons to get credit for the security fundamentals course. In this lesson, you will demonstrate your knowledge of operation security fundamentals.

OPSEC – Operational Security

- ★ OPSEC
- INFOSEC
- AT / FP

Reviewed, DIR-T USCGAUX



OPSEC – Operations Security

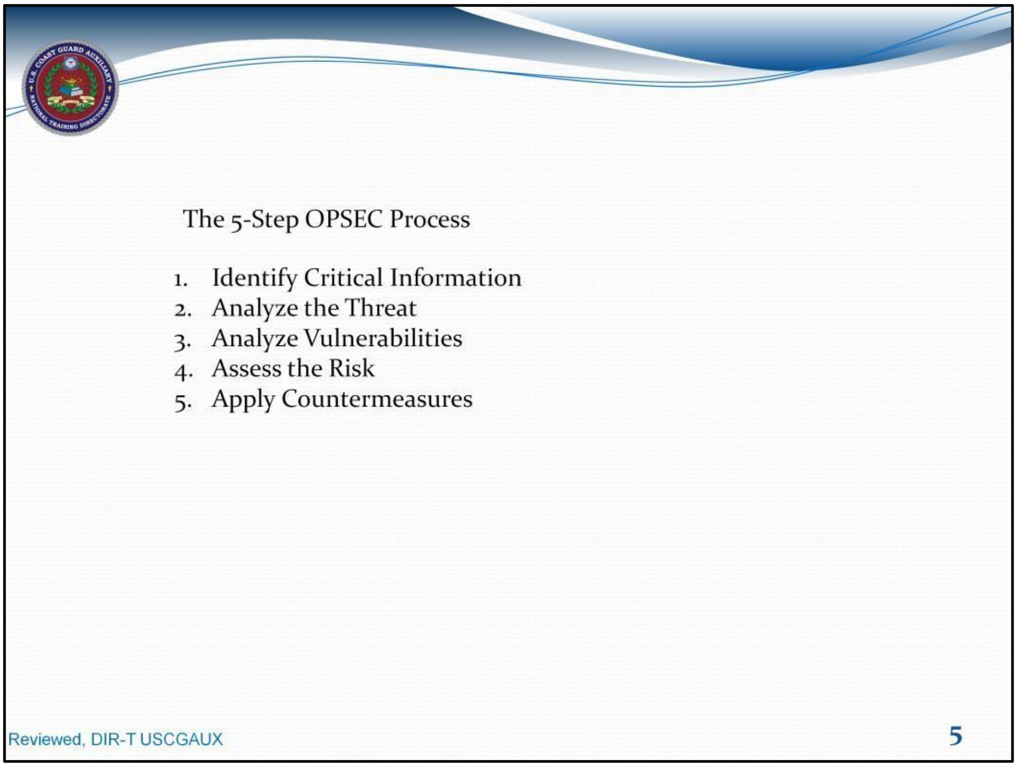
To successfully protect mission critical information, you need to be proficient in:

- Determining if information is critical.
- Evaluating threats.
- Evaluating vulnerabilities.
- Evaluating acceptable risk.
- Identifying countermeasures

Reviewed, DIR-T USCGAUX 4

Let’s start by defining OPSEC, or Operational Security. OPSEC, is an analytical process used to deny information generally unclassified from our adversaries, safeguards information concerning our intentions and capabilities by identifying, controlling and protecting indicators associated with our planning process or operations are exactly canceled you. you are vital in strengthening our upset posture by incorporating it into your daily activities.

OPSEC is a continual activity. The five step-by-step process helps individuals protect their pieces of the puzzle. Explore each of the steps for more information.

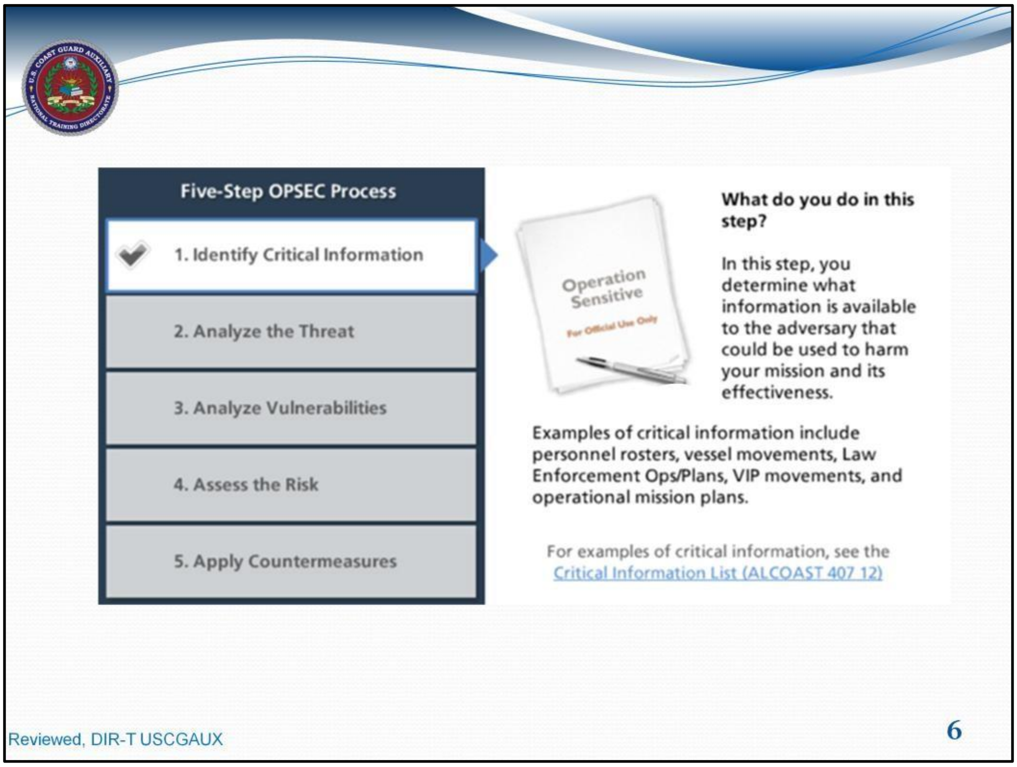


The 5-Step OPSEC Process

1. Identify Critical Information
2. Analyze the Threat
3. Analyze Vulnerabilities
4. Assess the Risk
5. Apply Countermeasures

Reviewed, DIR-T USCGAUX 5

Here is a look at the five-step OPSEC process.



Five-Step OPSEC Process

✓ 1. Identify Critical Information

2. Analyze the Threat

3. Analyze Vulnerabilities

4. Assess the Risk

5. Apply Countermeasures

What do you do in this step?

In this step, you determine what information is available to the adversary that could be used to harm your mission and its effectiveness.

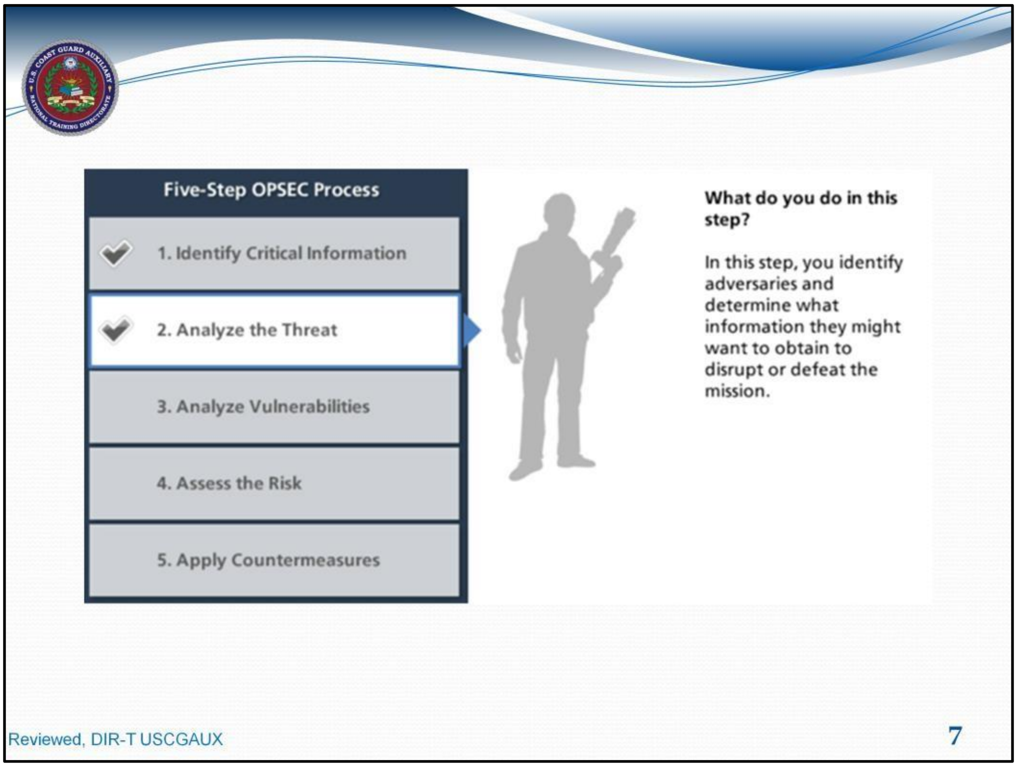
Examples of critical information include personnel rosters, vessel movements, Law Enforcement Ops/Plans, VIP movements, and operational mission plans.

For examples of critical information, see the Critical Information List (ALCOAST 407 12)

Reviewed, DIR-T USCGAUX

6

In order to understand OPSEC, you must first understand what needs to be protected. This information is referred to as critical information. Critical information is related to Coast Guard missions and operations, and is deemed sensitive enough that it requires a degree of protection. The Coast Guard critical information list is accessible from CG portal.



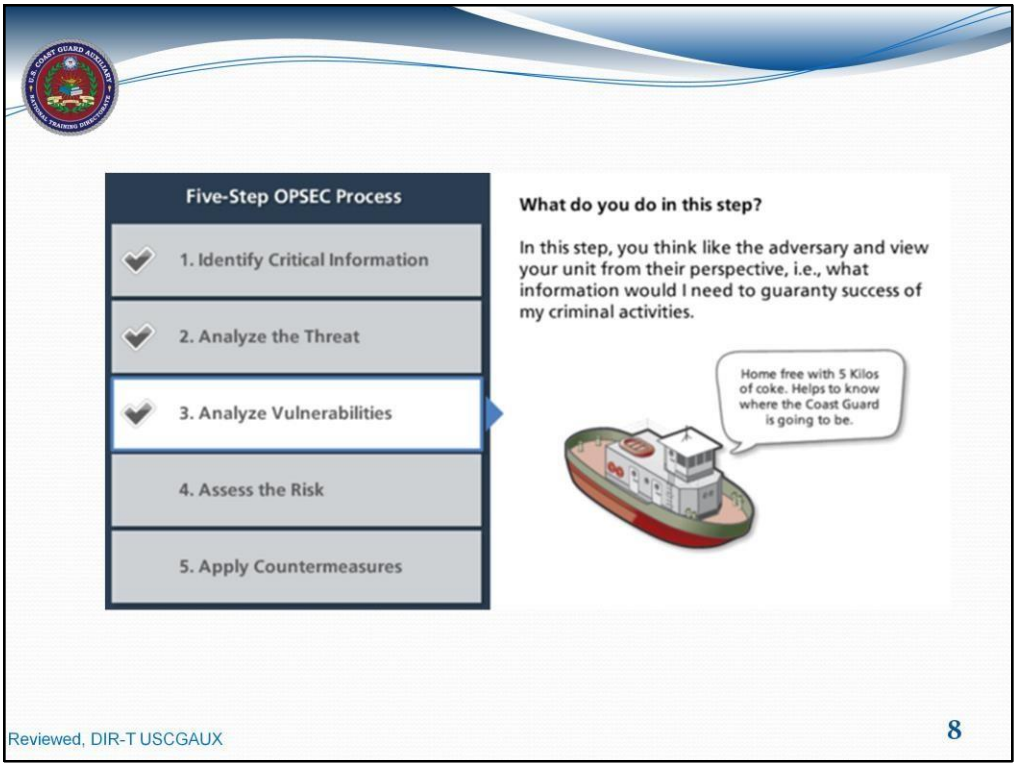
Five-Step OPSEC Process

- ✓ 1. Identify Critical Information
- ✓ 2. Analyze the Threat
- 3. Analyze Vulnerabilities
- 4. Assess the Risk
- 5. Apply Countermeasures

What do you do in this step?

In this step, you identify adversaries and determine what information they might want to obtain to disrupt or defeat the mission.

A threat is an adversary with intent and capability to target our critical information.



Five-Step OPSEC Process

- ✓ 1. Identify Critical Information
- ✓ 2. Analyze the Threat
- ✓ 3. Analyze Vulnerabilities
- 4. Assess the Risk
- 5. Apply Countermeasures

What do you do in this step?

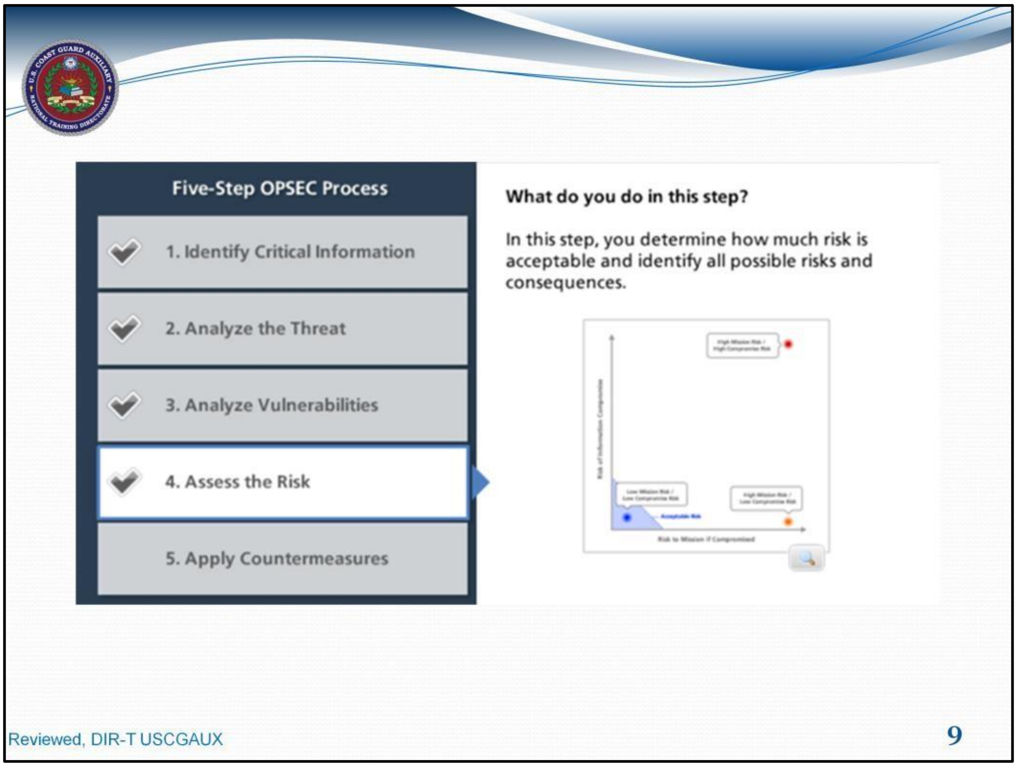
In this step, you think like the adversary and view your unit from their perspective, i.e., what information would I need to guaranty success of my criminal activities.

Home free with 5 Kilos of coke. Helps to know where the Coast Guard is going to be.

Reviewed, DIR-T USCGAUX

8

A vulnerability is a weakness that provides an adversary the opportunity to exploit your critical information.



Five-Step OPSEC Process

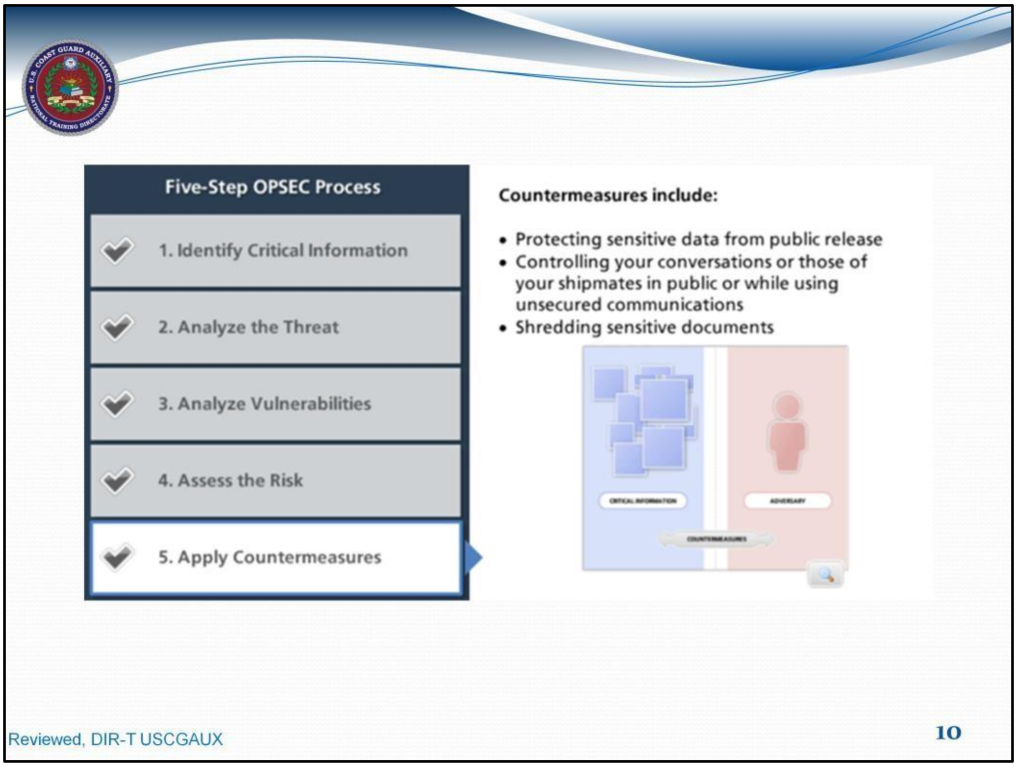
- ✓ 1. Identify Critical Information
- ✓ 2. Analyze the Threat
- ✓ 3. Analyze Vulnerabilities
- ✓ 4. Assess the Risk
- 5. Apply Countermeasures

What do you do in this step?

In this step, you determine how much risk is acceptable and identify all possible risks and consequences.

High Mission Risk / High Compromise Risk
Risk of Information Compromise
Low Mission Risk / Low Compromise Risk
Acceptable Risk
High Mission Risk / Low Compromise Risk
Risk to Mission if Compromised

Risk is the measure of the probability an adversary will be able to compromise your critical information while factoring the impact on your mission if they are successful.



Five-Step OPSEC Process

- ✓ 1. Identify Critical Information
- ✓ 2. Analyze the Threat
- ✓ 3. Analyze Vulnerabilities
- ✓ 4. Assess the Risk
- ✓ 5. Apply Countermeasures

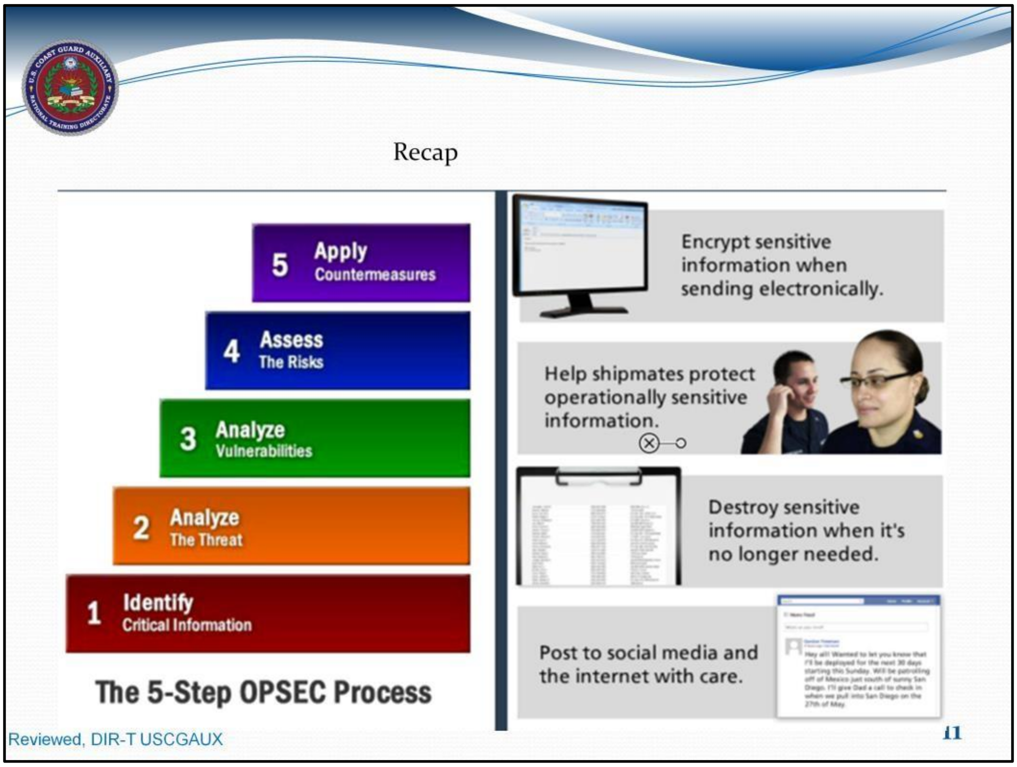
Countermeasures include:

- Protecting sensitive data from public release
- Controlling your conversations or those of your shipmates in public or while using unsecured communications
- Shredding sensitive documents

Reviewed, DIR-T USCGAUX

10

Countermeasures control, or hide indicators and reduce the adversary 's ability to exploit your vulnerabilities. By applying countermeasures, you reduce the risk.



Recap

5 Apply
Countermeasures
4 Assess
The Risks
3 Analyze
Vulnerabilities
2 Analyze
The Threat
1 Identify
Critical Information

The 5-Step OPSEC Process

Encrypt sensitive information when sending electronically.

Help shipmates protect operationally sensitive information.

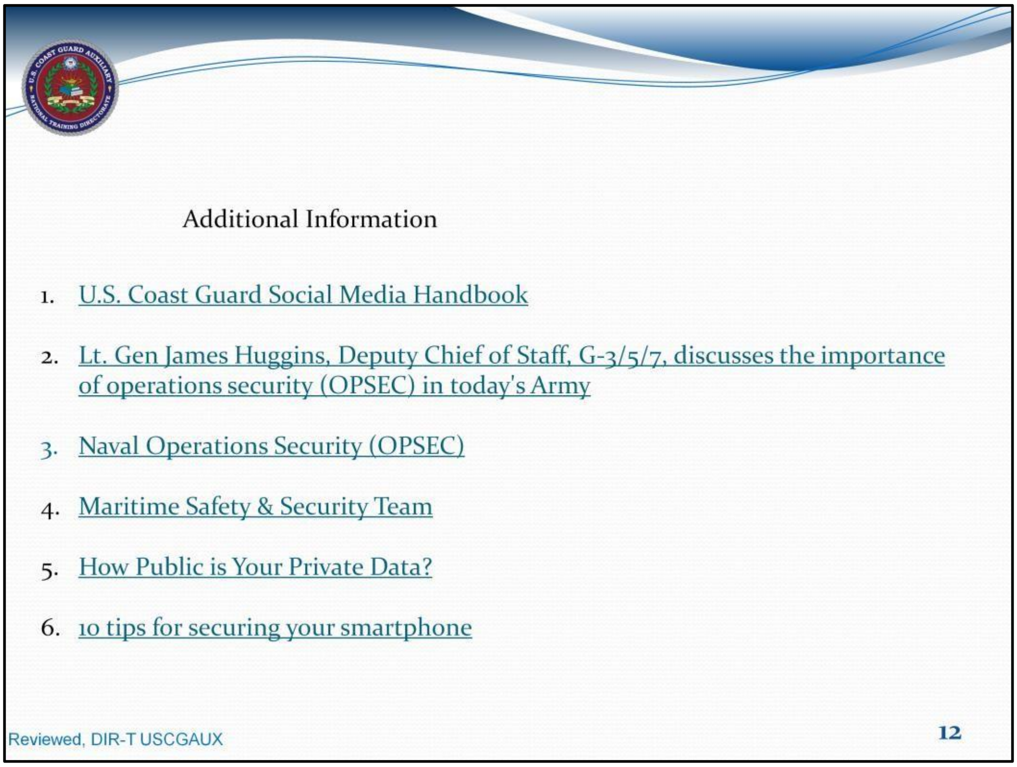
Destroy sensitive information when it's no longer needed.

Post to social media and the internet with care.

Hey all! Wanted to let you know that I'll be deployed for the next 30 days starting this Sunday. Will be patrolling off of Mexico just south of sunny San Diego. I'll give Dad a call to check in when we pull into San Diego on the 27th of May.

Reviewed, DIR-T USCGAUX

In this lesson we covered the 5 step OPSEC process. It is essential that you understand the basic steps of the OPSEC process and how to apply them. Practicing good OPSEC helps protect Coast Guard missions and people.



Additional Information

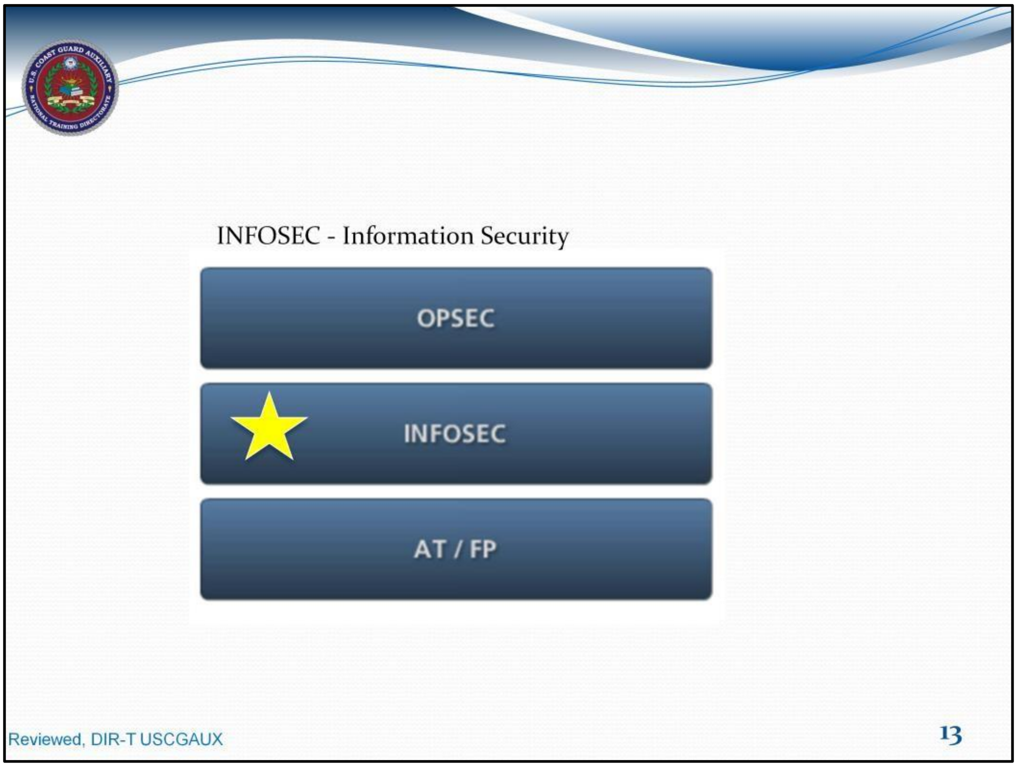
1. U.S. Coast Guard Social Media Handbook
2. Lt. Gen James Huggins, Deputy Chief of Staff, G-3/5/7, discusses the importance of operations security (OPSEC) in today's Army
3. Naval Operations Security (OPSEC)
4. Maritime Safety & Security Team
5. How Public is Your Private Data?
6. 10 tips for securing your smartphone

Reviewed, DIR-T USCGAUX

12

Additional Information

1. http://www.dvidshub.net/publication/issues/10409
2. https://www.youtube.com/watch?v=WhG6e_NRczs
3. https://www.facebook.com/NavalOPSEC
4. https://www.youtube.com/watch?v=QEgQ4LTBAEQ
5. http://www.whoishostingthis.com/blog/2014/11/12/public-private-data/
6. https://nakedsecurity.sophos.com/2013/10/08/10-tips-for-securing-your-smartphone/



INFOSEC - Information Security

OPSEC

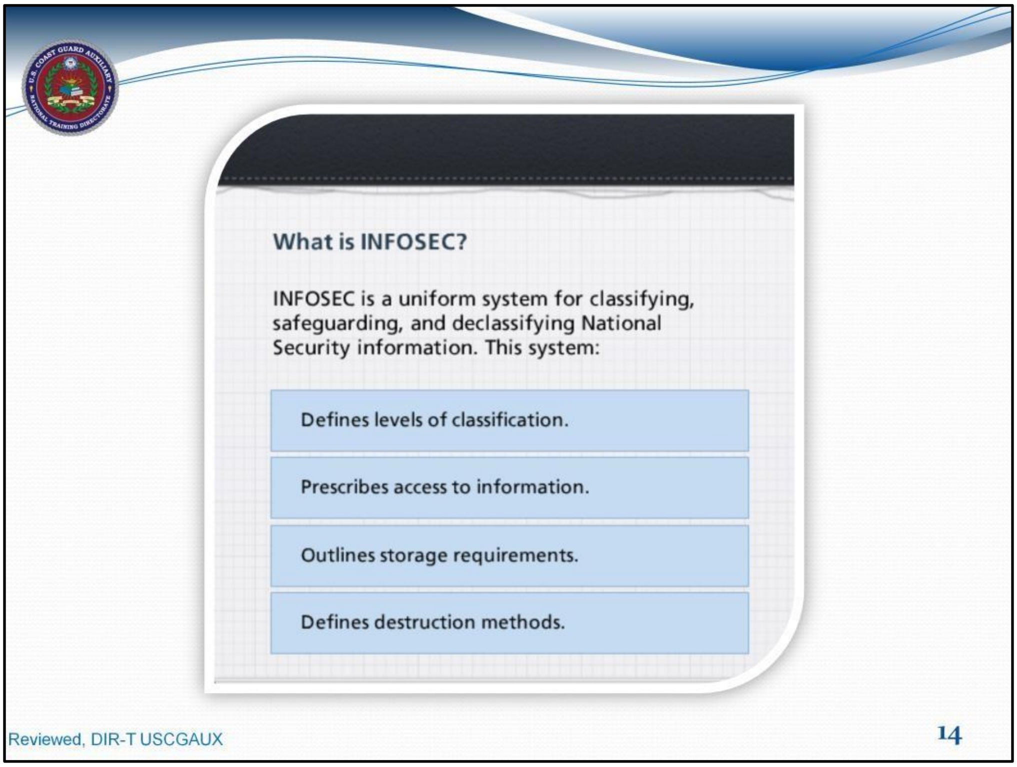
★ INFOSEC

AT / FP

Reviewed, DIR-T USCGAUX

13

In this section, we’ll review the fundamentals of information security,



What is INFOSEC?

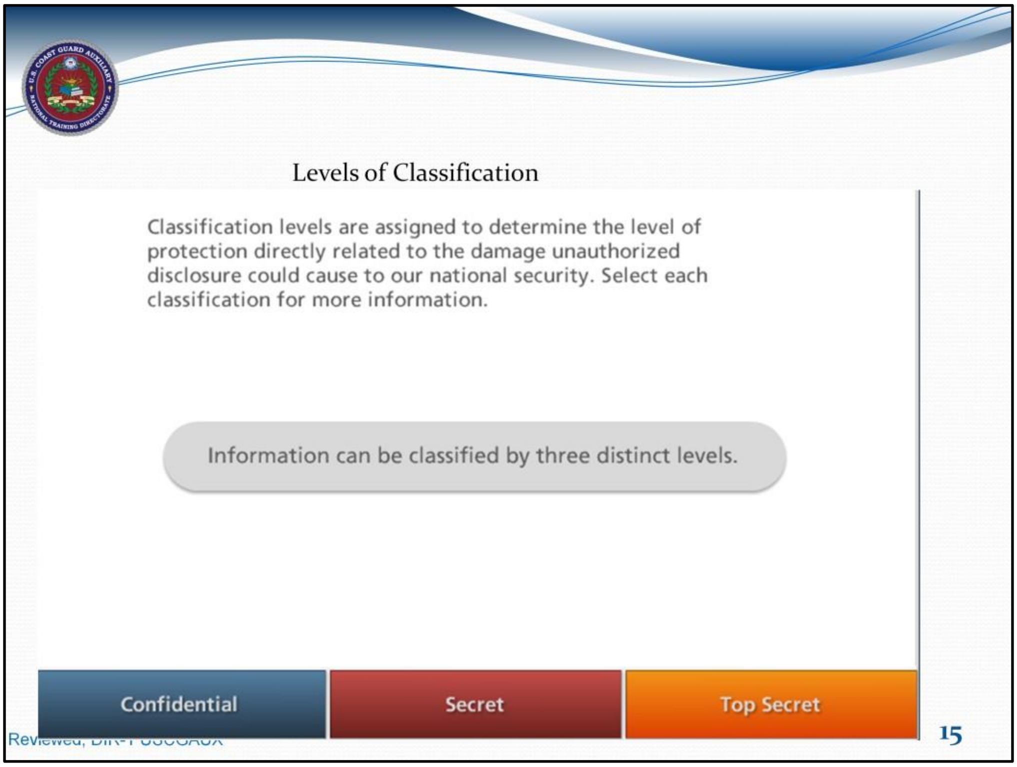
INFOSEC is a uniform system for classifying, safeguarding, and declassifying National Security information. This system:

- Defines levels of classification.
- Prescribes access to information.
- Outlines storage requirements.
- Defines destruction methods.

Reviewed, DIR-T USCGAUX

14

Information security or INFOSEC is a program that prescribes a uniform system for classifying, safeguarding, and declassifying National Security information. The INFOSEC program defines levels of classification for National Security information including confidential, secret and top-secret. The program also defines access storage, declassification, and destruction requirements.

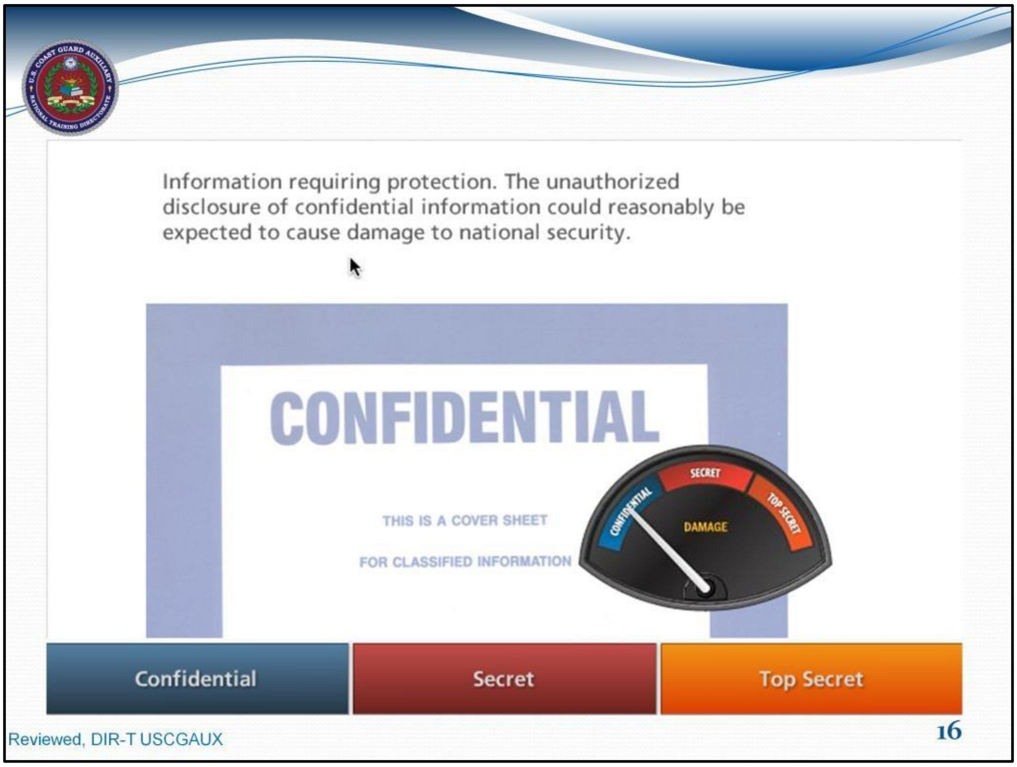


Levels of Classification

Classification levels are assigned to determine the level of protection directly related to the damage unauthorized disclosure could cause to our national security. Select each classification for more information.

Information can be classified by three distinct levels.

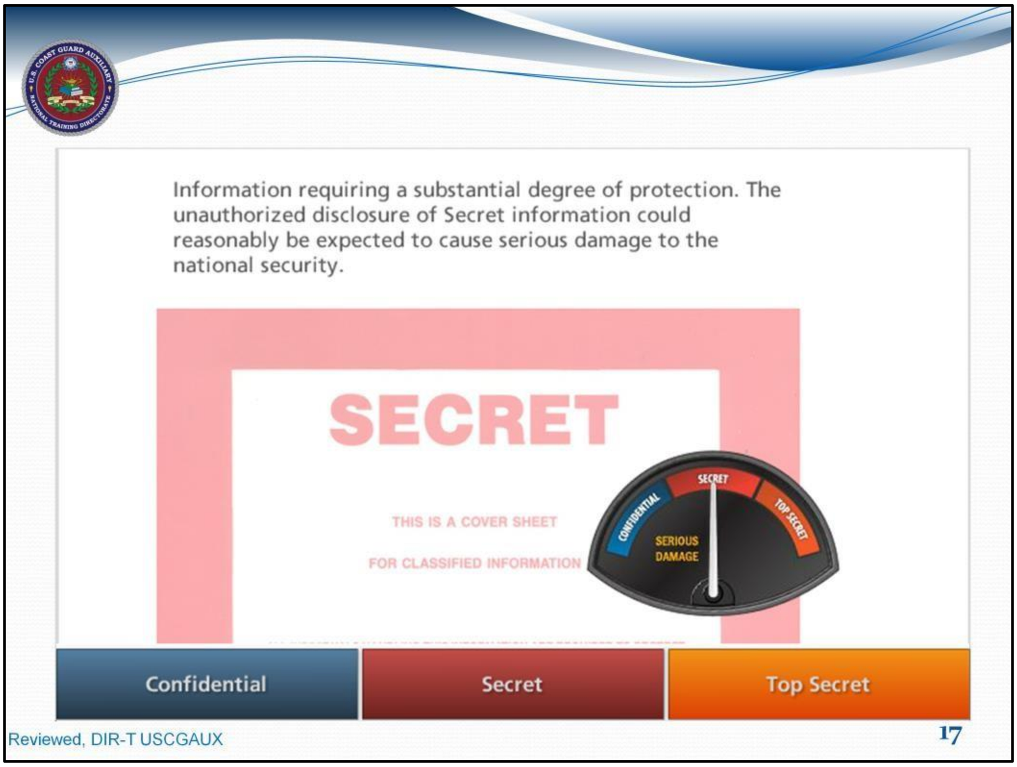
You need to be familiar with the three levels of information classified in the interest of National Security. Select each classification for more information.



Information requiring protection. The unauthorized disclosure of confidential information could reasonably be expected to cause damage to national security.

Reviewed, DIR-T USCGAUX

Confidential information is information requiring protection. The unauthorized disclosure of confidential information could reasonably be expected to cause damage to national security

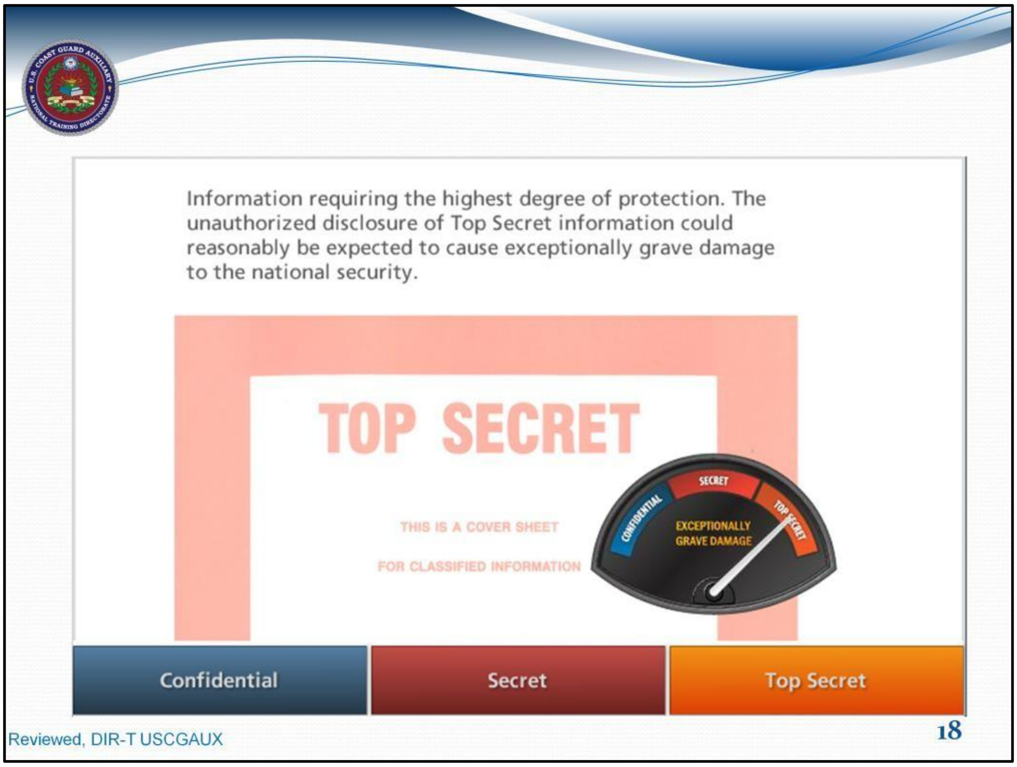


Information requiring a substantial degree of protection. The unauthorized disclosure of Secret information could reasonably be expected to cause serious damage to the national security.

Reviewed, DIR-T USCGAUX

17

Secret information requires a substantial degree of protection. The unauthorized disclosure of Secret information could reasonably be expected to cause serious damage to national security.

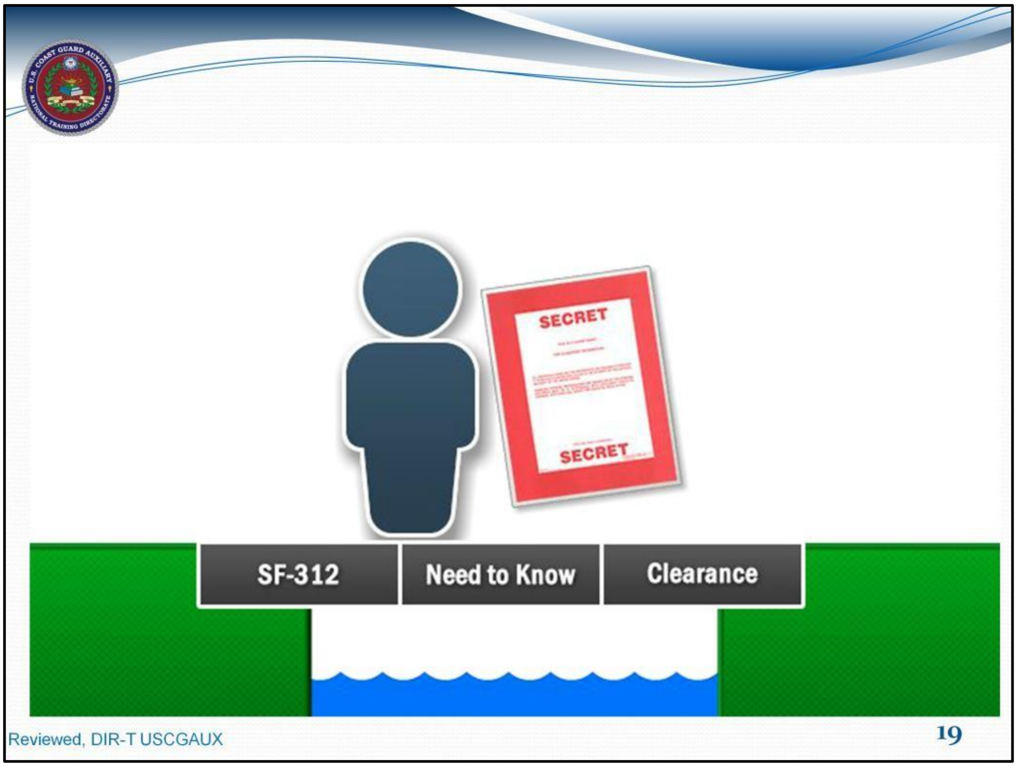


Information requiring the highest degree of protection. The unauthorized disclosure of Top Secret information could reasonably be expected to cause exceptionally grave damage to the national security.

Reviewed, DIR-T USCGAUX

18

Top-secret information is information requiring the highest degree of protection. The unauthorized disclosure of top-secret information could reasonably be expected to cause exceptionally grave damage to the national security.



SF-312 | Need to Know | Clearance

Reviewed, DIR-T USCGAUX

What must you have in order to access classified information?

First, you need security clearance.

Second, you must have a valid need to know meaning your official duties require knowledge or possession of the information

And lastly, you must have a properly executed SF-312, classified information nondisclosure agreement. No SF-312, no need to know, no security clearance, means no access to classified information.

Confidential and Secret information is stored in a approved container, vault, or secure room.

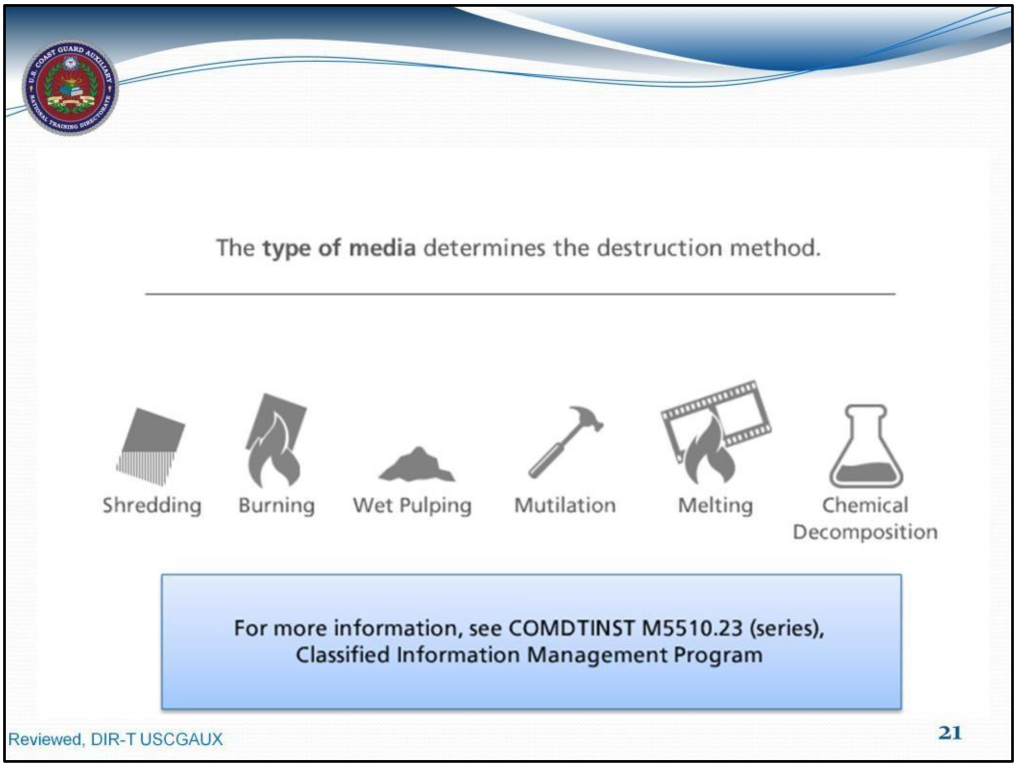
Top Secret information **also** requires supplemental controls (alarm, guard.)

Reviewed, DIR-T USCGAUX

20

What are the requirements for storage and safeguarding classified information?

Classified materials must be stored in an approved container or secure room. Classified material marked top secret must also have additional supplemental control, such as a guard or alarm system.



The **type of media** determines the destruction method.

Shredding Burning Wet Pulping Mutilation Melting Chemical Decomposition

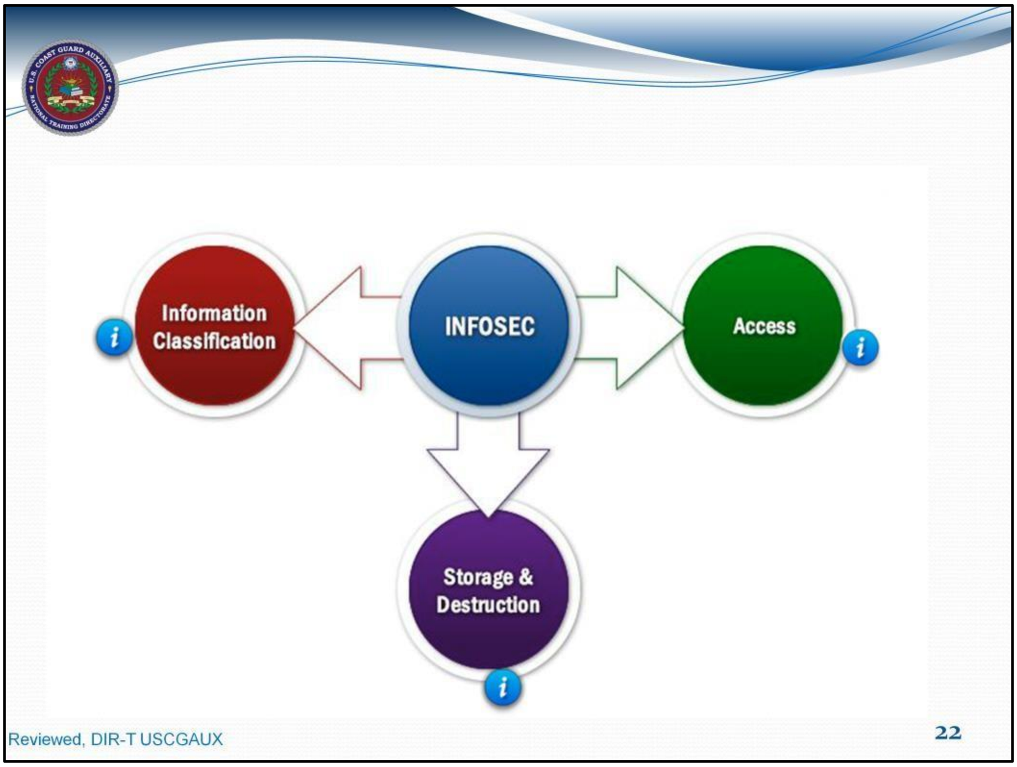
For more information, see COMDTINST M5510.23 (series), Classified Information Management Program

Reviewed, DIR-T USCGAUX

21

Approved methods of destruction prevent reconstitution of information from physical media. Several methods are defined in the classified information management program,

These methods include crosscut shredding with a residue particle size of one millimeter by five millimeter, burning, wet pulping, mutilation and melting, and chemical decomposition.



Information Classification

INFOSEC

Access

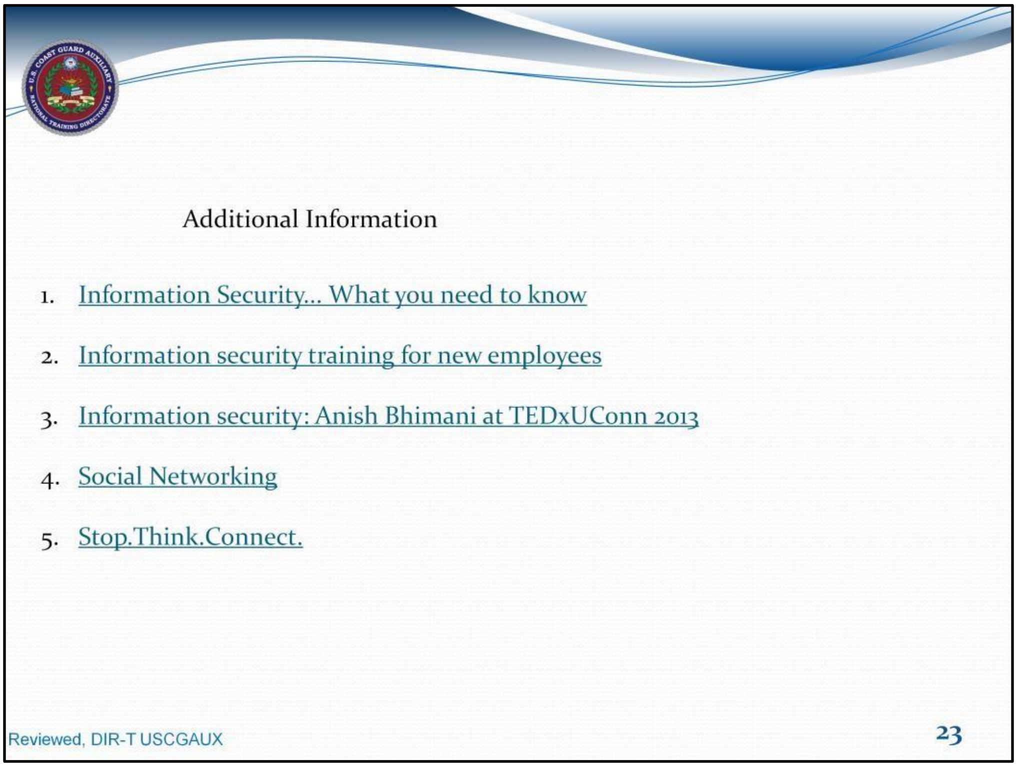
Storage & Destruction

Reviewed, DIR-T USCGAUX

22

Let's review your role in INFOSEC. Classified materials are designated on three levels, confidential, secret and top-secret; access to classified materials requires three things: a security clearance that meets or exceeds the classification level of the document, a need to know and the properly executed nondisclosure agreement. Classified materials must be stored in a GSA approved lock container. Top-secret materials must also be protected by an alarm or guarded facility. See the classified information management program you have any questions regarding identification access to storage or destruction of classified information.

If you have any questions regarding information security don't hesitate to ask you units command security officer or CSO.

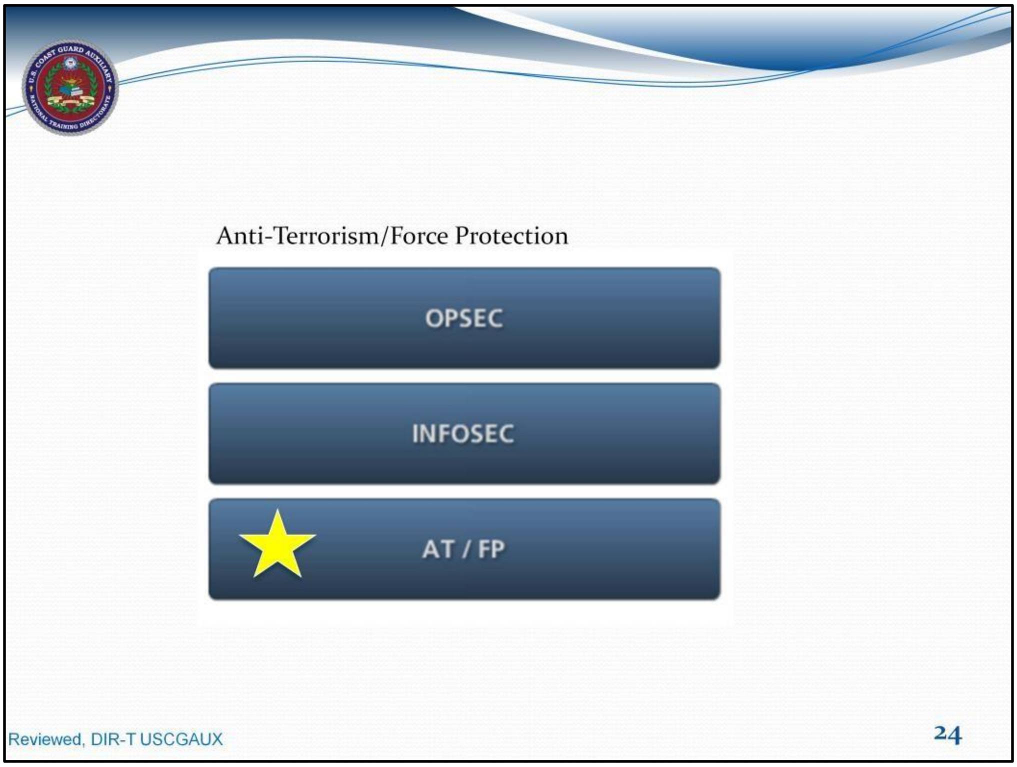


Additional Information

1. Information Security… What you need to know
2. Information security training for new employees
3. Information security: Anish Bhimani at TEDxUConn 2013
4. Social Networking
5. Stop.Think.Connect.

Reviewed, DIR-T USCGAUX

Additional Information

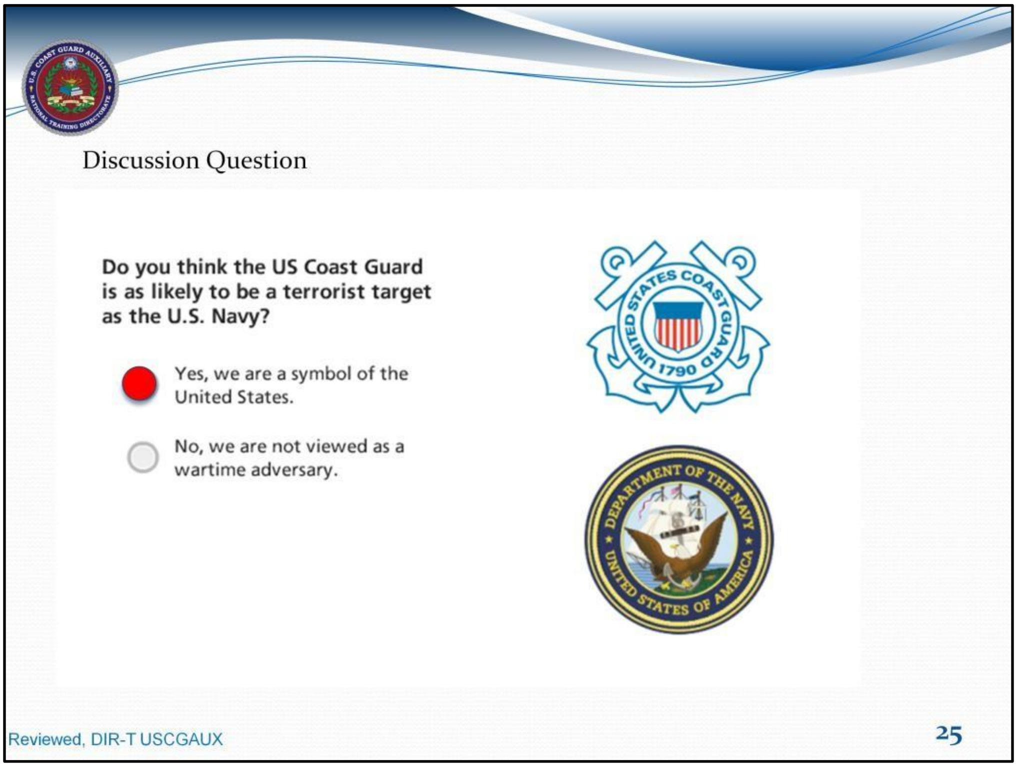


Anti-Terrorism/Force Protection

OPSEC

INFOSEC

★ AT / FP



Discussion Question

Do you think the US Coast Guard is as likely to be a terrorist target as the U.S. Navy?

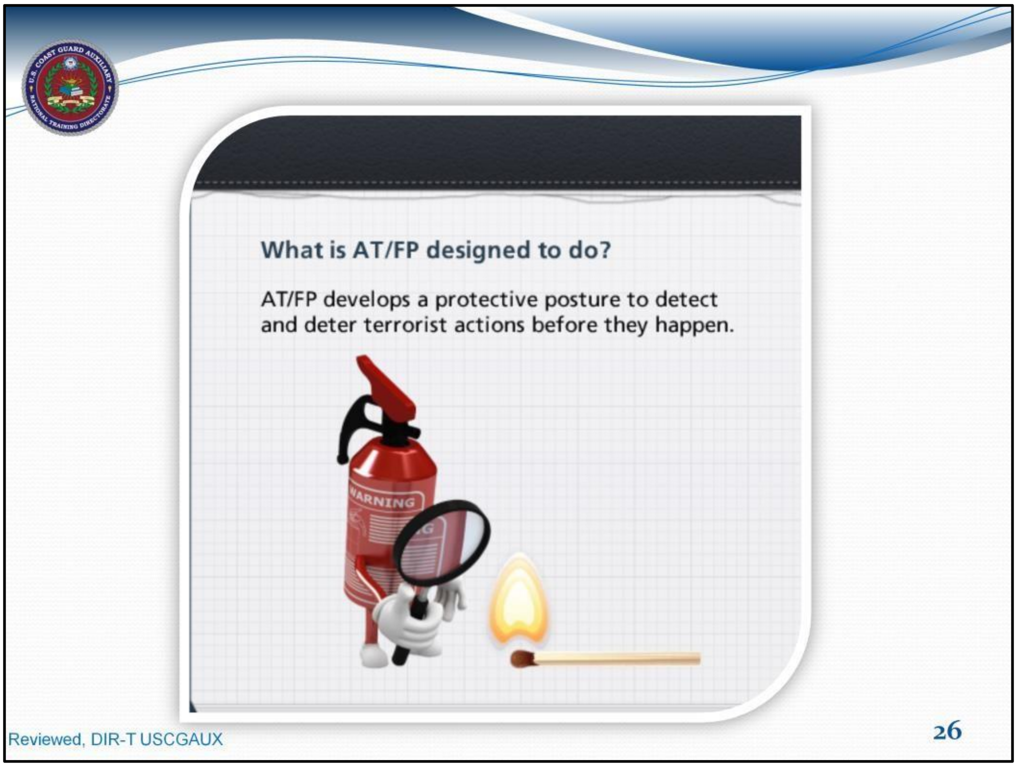
● Yes, we are a symbol of the United States.

○ No, we are not viewed as a wartime adversary.

Reviewed, DIR-T USCGAUX

25

Question: Do you think the Coast Guard is a likely target for Foreign terrorist? We are a symbol of the US, with high visibility and high profile.



What is AT/FP designed to do?

AT/FP develops a protective posture to detect and deter terrorist actions before they happen.

Reviewed, DIR-T USCGAUX

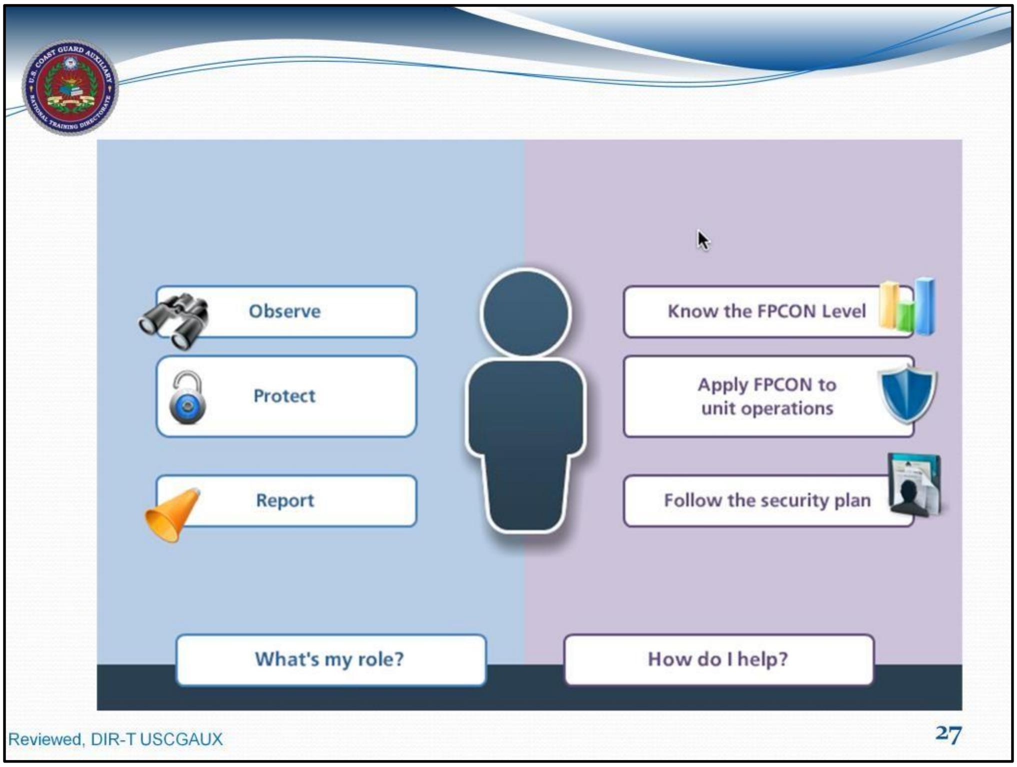
26

It’s important to understand generally what types of targets terrorists choose and why. A Coast Guard cutter could be a possible terrorist target. Because it is a high profile, high visibility, indirectly symbolizes the United States. You as a member of the armed services are also a potential terrorist target.

Anti-terrorism and force protection or AT/FP establishes uniform procedures and measures for use in responding to progressive levels of terrorist threats to Coast Guard units, both ashore and afloat.

AT/FP is designed to develop a protective posture in peacetime that will carry over if an attack were actually to occur.

AT/FP also includes procedures that are intended to protect and deter planned terrorist actions before they take place, thereby reducing the probability of a terrorist event.



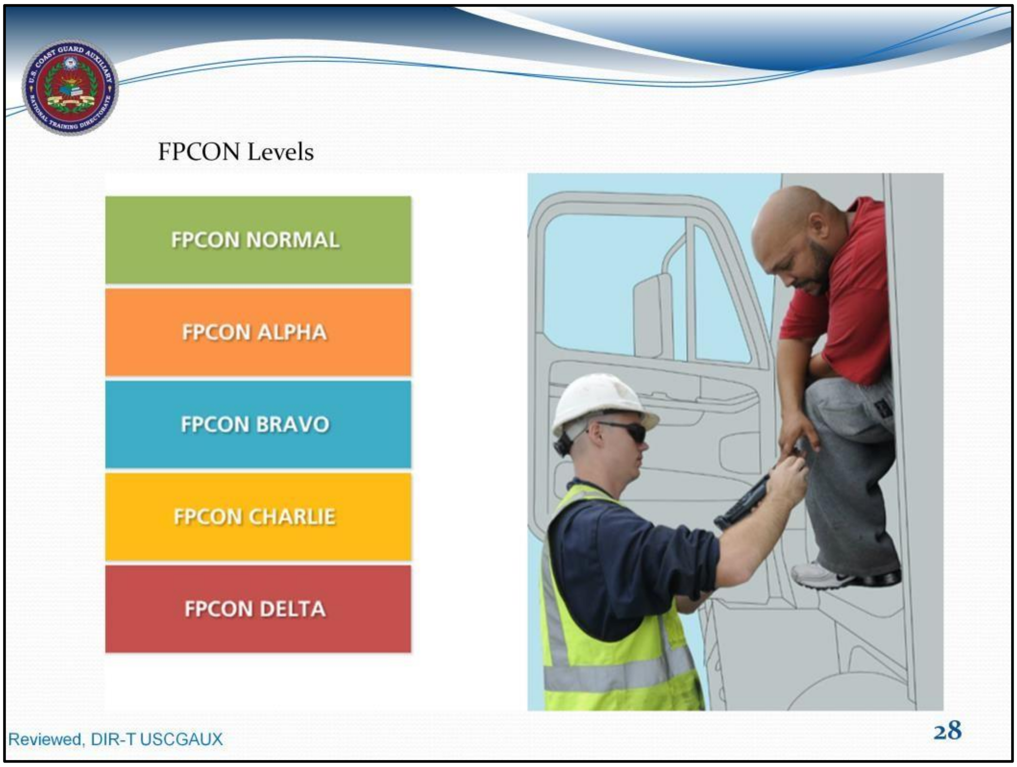
You can follow three simple steps in your role in the AT/FP program at your unit.

One: Observe, be aware of your surroundings. In your daily routine, you are the eyes and ears of the AT/FP program. Don't ignore unusual activities.

Two: Protect, in some instances you may be able to take action to prevent terrorist actions. In extreme cases, if you our your unit is being targeted do not hesitate to take action

Three: Report, never hesitate to report suspicious activity or something that seems out of place. You should contact a supervisor, the command security officer, security or police, as appropriate.

You should always know your units force protection condition or FPCON. Be aware when it changes and be ready to discuss what the condition means to unit operations. Follow your unit security plan. A force protection condition is a DOD approved system for standardizing the identification recommended preventative actions and responses to terrorist threats against US personnel and facilities.



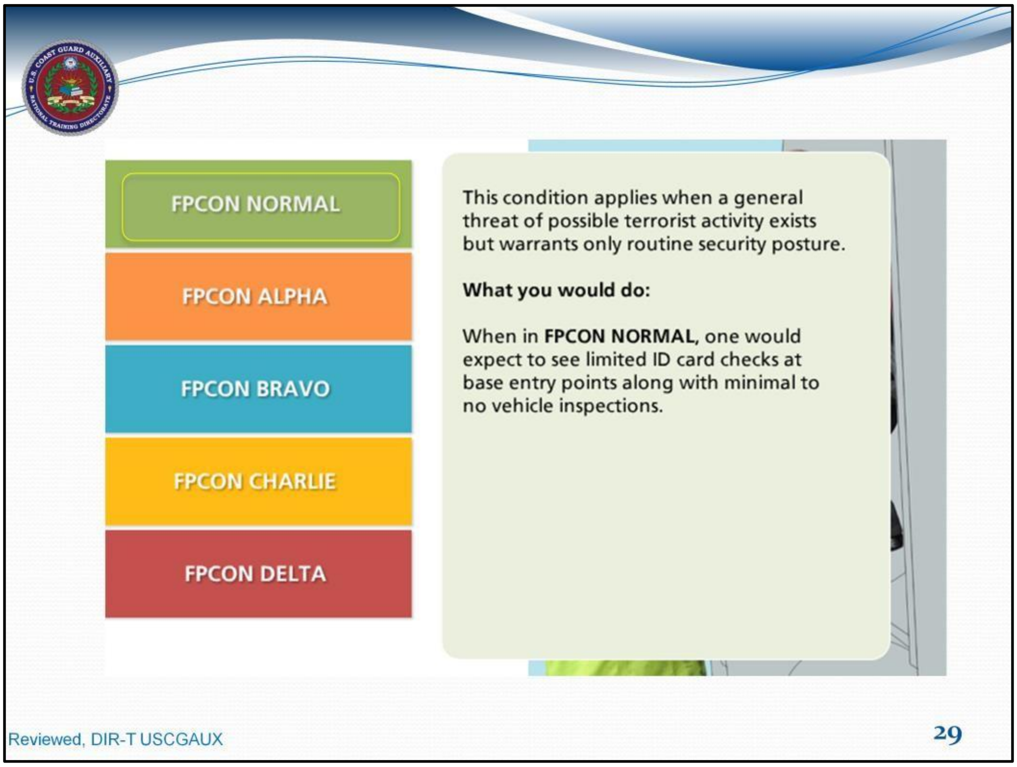
FPCON Levels

- FPCON NORMAL
- FPCON ALPHA
- FPCON BRAVO
- FPCON CHARLIE
- FPCON DELTA

Reviewed, DIR-T USCGAUX

28

There are five FPCON levels. Let’s review eachone.



FPCON NORMAL

FPCON ALPHA

FPCON BRAVO

FPCON CHARLIE

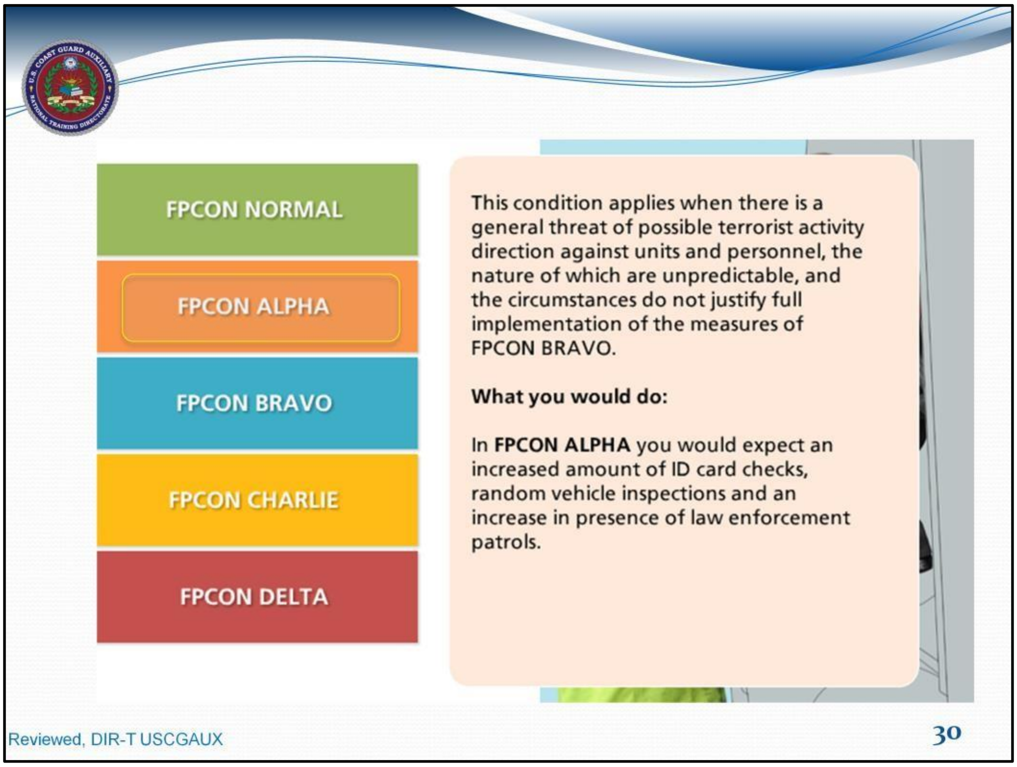
FPCON DELTA

This condition applies when a general threat of possible terrorist activity exists but warrants only routine security posture.

What you would do:

When in **FPCON NORMAL**, one would expect to see limited ID card checks at base entry points along with minimal to no vehicle inspections.

Reviewed, DIR-T USCGAUX



FPCON NORMAL

FPCON ALPHA

FPCON BRAVO

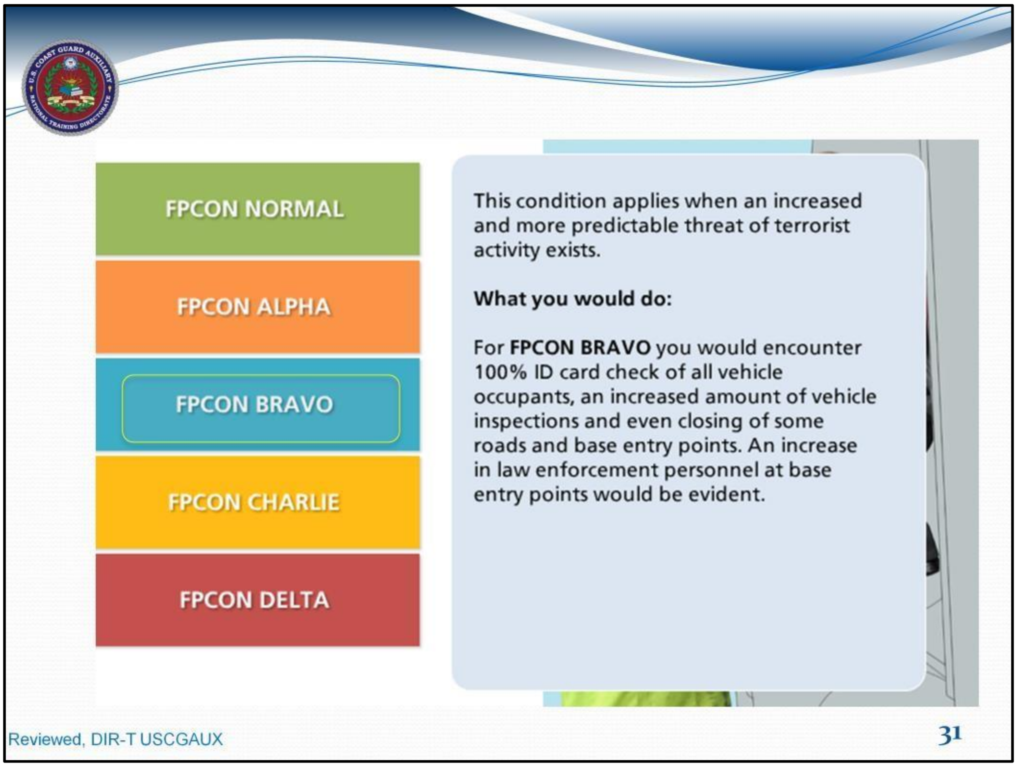
FPCON CHARLIE

FPCON DELTA

This condition applies when there is a general threat of possible terrorist activity direction against units and personnel, the nature of which are unpredictable, and the circumstances do not justify full implementation of the measures of FPCON BRAVO.

What you would do:

In **FPCON ALPHA** you would expect an increased amount of ID card checks, random vehicle inspections and an increase in presence of law enforcement patrols.



FPCON NORMAL

FPCON ALPHA

FPCON BRAVO

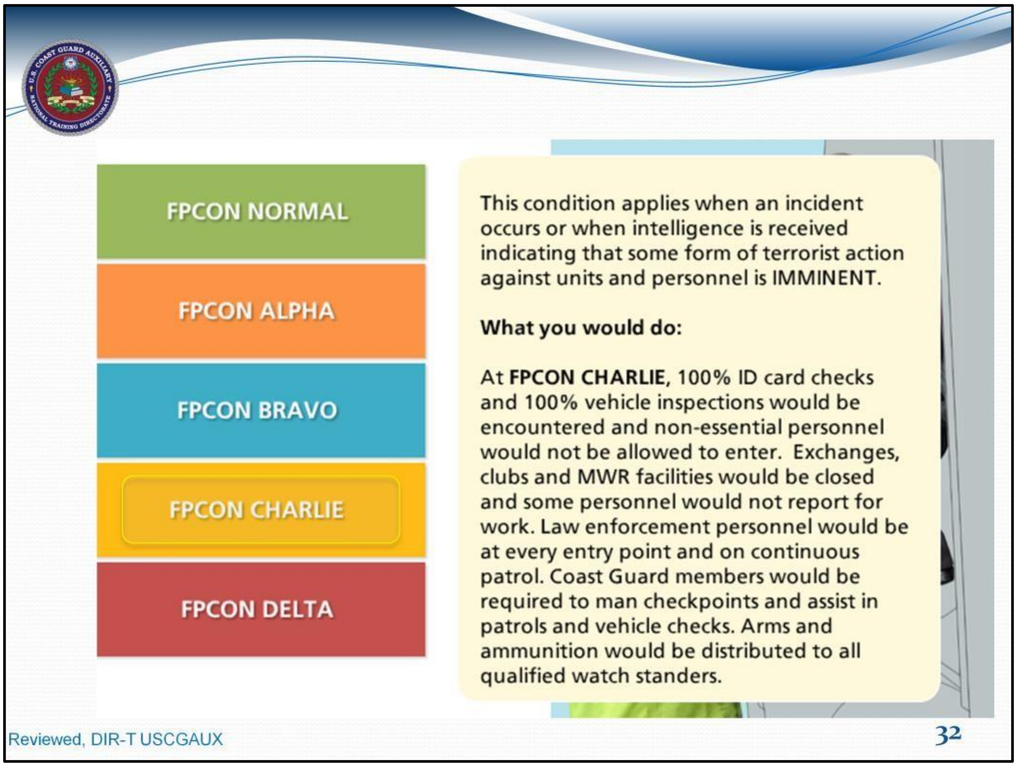
FPCON CHARLIE

FPCON DELTA

This condition applies when an increased and more predictable threat of terrorist activity exists.

What you would do:

For **FPCON BRAVO** you would encounter 100% ID card check of all vehicle occupants, an increased amount of vehicle inspections and even closing of some roads and base entry points. An increase in law enforcement personnel at base entry points would be evident.



FPCON NORMAL

FPCON ALPHA

FPCON BRAVO

FPCON CHARLIE

FPCON DELTA

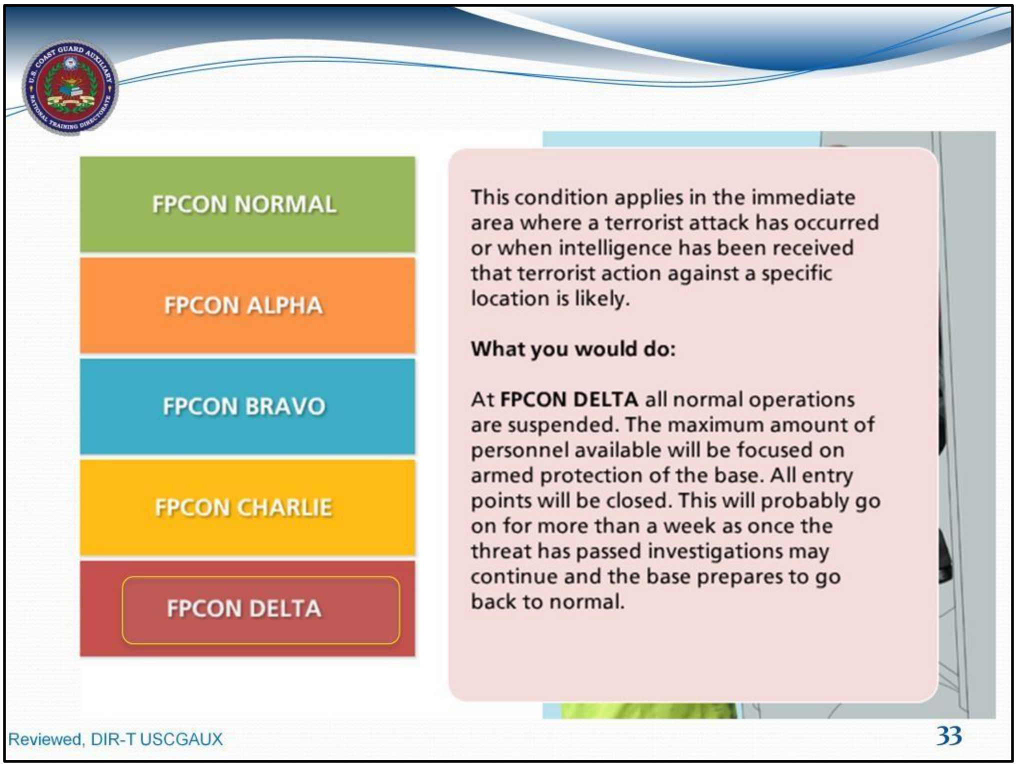
This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against units and personnel is IMMINENT.

What you would do:

At **FPCON CHARLIE**, 100% ID card checks and 100% vehicle inspections would be encountered and non-essential personnel would not be allowed to enter. Exchanges, clubs and MWR facilities would be closed and some personnel would not report for work. Law enforcement personnel would be at every entry point and on continuous patrol. Coast Guard members would be required to man checkpoints and assist in patrols and vehicle checks. Arms and ammunition would be distributed to all qualified watch standers.

Reviewed, DIR-T USCGAUX

32



FPCON NORMAL

FPCON ALPHA

FPCON BRAVO

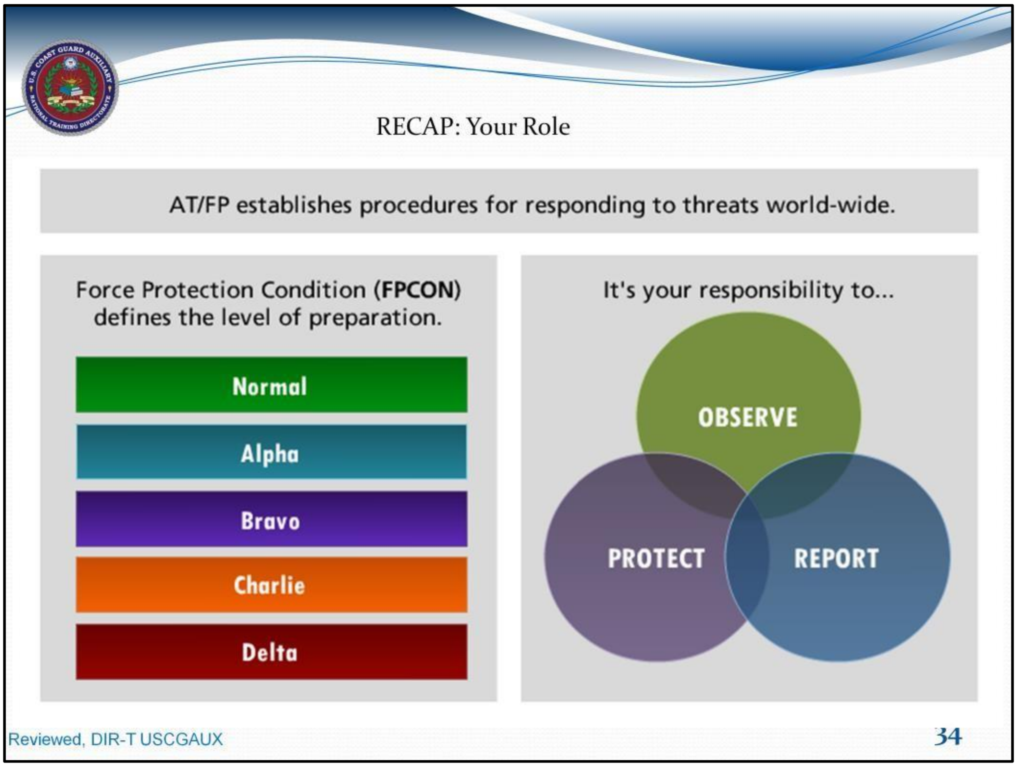
FPCON CHARLIE

FPCON DELTA

This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely.

What you would do:

At **FPCON DELTA** all normal operations are suspended. The maximum amount of personnel available will be focused on armed protection of the base. All entry points will be closed. This will probably go on for more than a week as once the threat has passed investigations may continue and the base prepares to go back to normal.



RECAP: Your Role

AT/FP establishes procedures for responding to threats world-wide.

Force Protection Condition (**FPCON**) defines the level of preparation.

- Normal
- Alpha
- Bravo
- Charlie
- Delta

It's your responsibility to...

OBSERVE

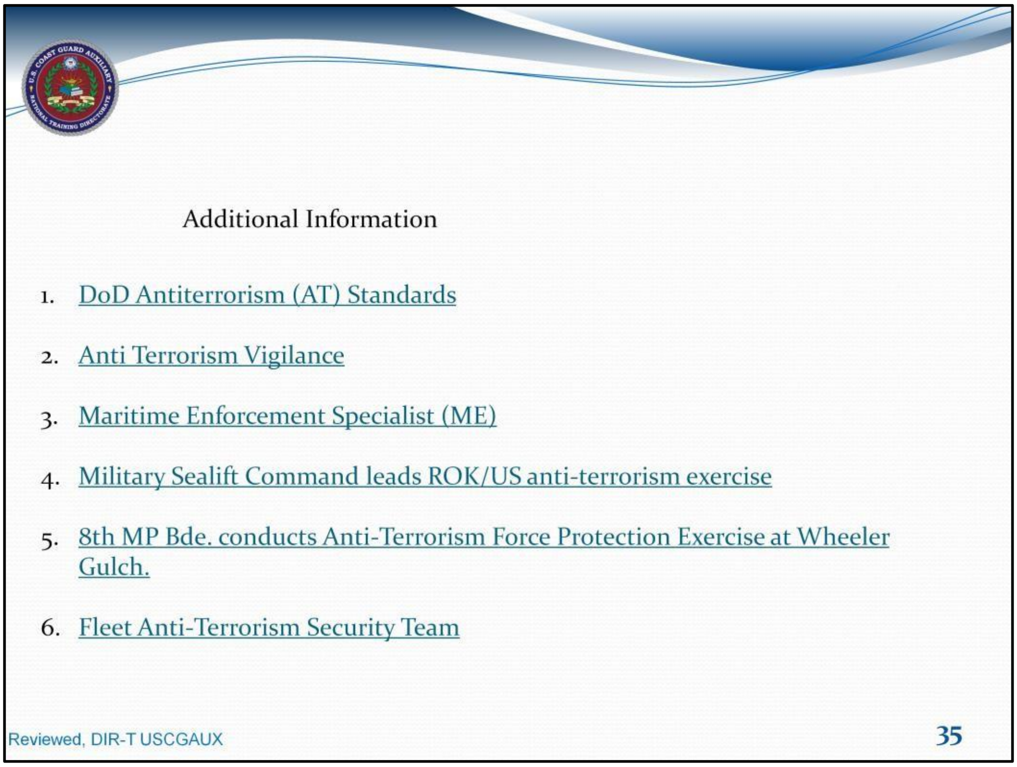
PROTECT

REPORT

Reviewed, DIR-T USCGAUX

let's review your role in antiterrorism and force protection, AT/FP establishes a protective posture for units worldwide. this program establishes procedures for responding to progressive threat levels preparations in response to threat.

Levels are defined by five separate force protection conditions normal Alpha, Bravo, Charlie and Delta which are defined levels for your preparation or increasing risks of attack US government agency. We are a target and rely on the vigilance of every shipmate to observe the tech and report any situation seems out of the ordinary



Additional Information

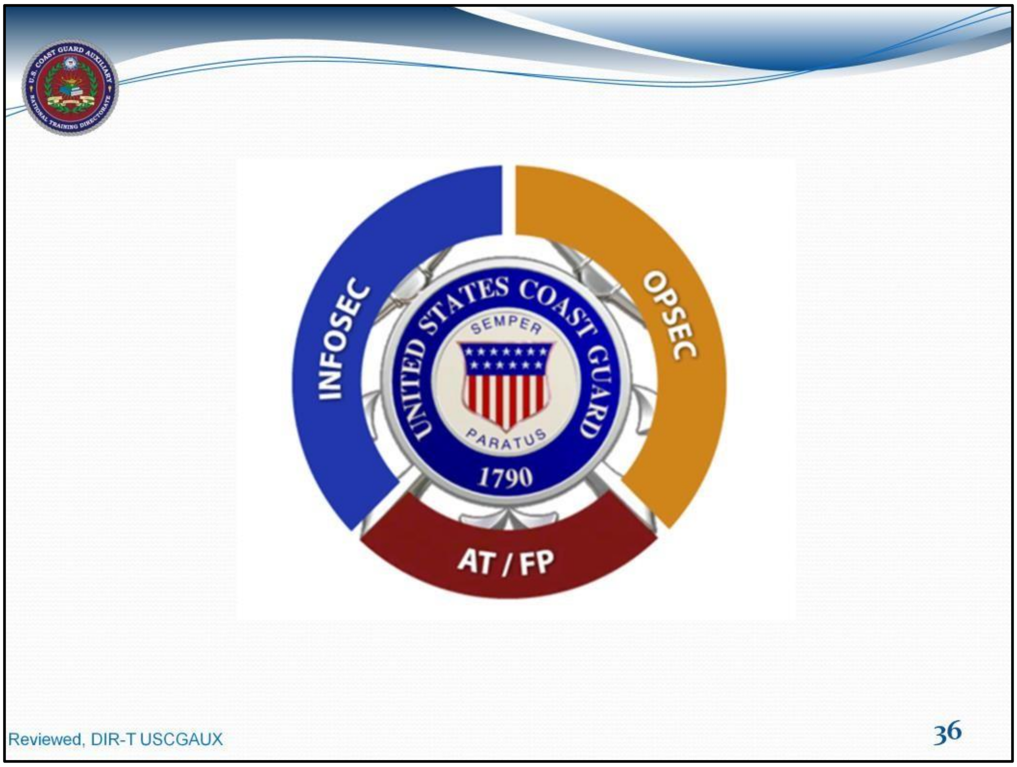
1. DoD Antiterrorism (AT) Standards
2. Anti Terrorism Vigilance
3. Maritime Enforcement Specialist (ME)
4. Military Sealift Command leads ROK/US anti-terrorism exercise
5. 8th MP Bde. conducts Anti-Terrorism Force Protection Exercise at Wheeler Gulch.
6. Fleet Anti-Terrorism Security Team

Reviewed, DIR-T USCGAUX

35

Additional Information

1. http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf
2. https://www.youtube.com/watch?v=mybVTQROV0s
3. https://www.youtube.com/watch?v=8ALY06ixvc4
4. https://www.youtube.com/watch?v=Rn671Wk4EQ8
5. http://vimeo.com/71951550
6. https://www.youtube.com/watch?v=ol7U8FOC9Lg



INFOSEC

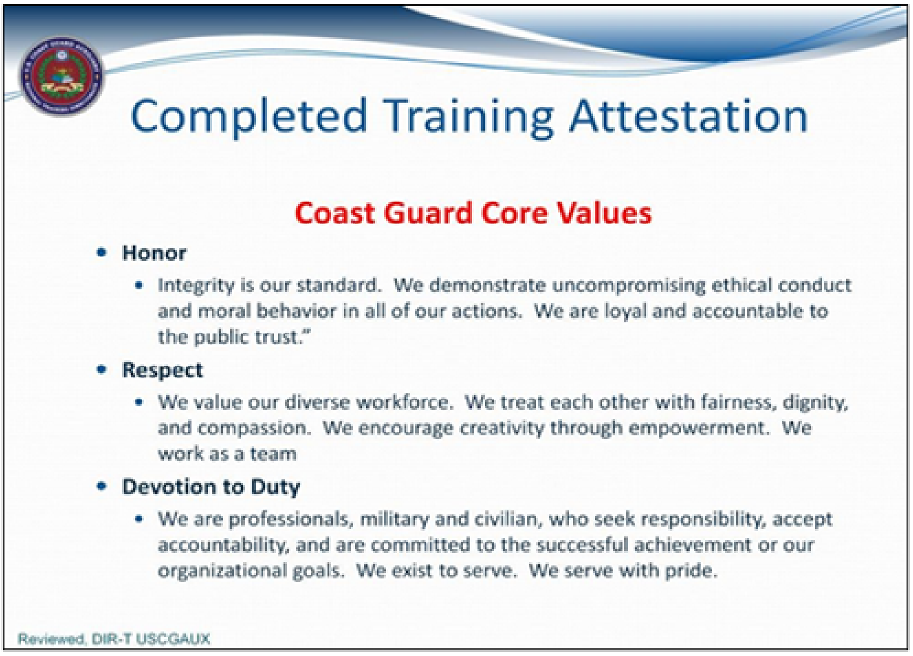
OPSEC

AT / FP

Reviewed, DIR-T USCGAUX

36

As a member of the US Coast Guard Auxiliary you play an important role in ensuring security and maintaining readiness, OPSEC, INFOSEC and AntiTerrorism Force Protection programs are in place to protect operational capabilities, national security information, and most importantly the safety and security of all Coast Guard personnel. This training has provided a fundamental overview of the practices and procedures associated with OPSEC, INFOSEC and AT/FP. Your journey does not stop here. Your continued vigilance is the key to security success.



Completed Training Attestation

Coast Guard Core Values

- **Honor**
  - Integrity is our standard. We demonstrate uncompromising ethical conduct and moral behavior in all of our actions. We are loyal and accountable to the public trust."
- **Respect**
  - We value our diverse workforce. We treat each other with fairness, dignity, and compassion. We encourage creativity through empowerment. We work as a team
- **Devotion to Duty**
  - We are professionals, military and civilian, who seek responsibility, accept accountability, and are committed to the successful achievement or our organizational goals. We exist to serve. We serve with pride.

Reviewed, DIR-T USCGAUX

The mandatory training that you have just completed reflects the ***Core Values of the U.S. Coast Guard*** and ***Coast Guard Auxiliary***. As a member of this organization, you have taken an oath to uphold those Core Values. In order to receive completion credit for this training, please read, understand, and sign this document. Once completed, keep a copy for your records and provide a copy to your Flotilla Staff Officer for Information Services (FSO-IS) for AUXDATA entry.

In regards to the selected mandated training modules: Codes: ______________________________

I,____(print name) as a member of District______

Division____Flotilla_______attest that I have completed and understand the course contents.

Signature:____, Member ID _______________

Date: ____________________

Course Code	Course Name	Frequency
502379	Building Resilience and Preventing Suicide	Every 5 years
810030	Security Fundamentals	Every 5 years
810015	Privacy at DHS / Protecting Personal Information	Every 5 years
810000	Sexual Harassment Prevention	Every 5 years
810045	Sexual Assault Prevention and Response	Every 5 years
502319	Civil Rights Awareness	Every 5 years
502306	Ethics 1 / Personal Gifts	1 time only
502290	Influenza Training	1 time only