iWATCH, OPSEC and Information Security Awareness Training
Objectives

Following completion of this module, participants will be able to:

• Develop a greater understanding of the iWATCH Initiative and their roles as contractors working in a government facility
• Develop a greater awareness of OPSEC and the identified strategies for properly securing and maintaining personal information on Child and Youth Program participants
• Identifying the best strategies for safe-guarding government equipment, information and reports
THE iWATCH INITIATIVE
As a result of recent attacks and breeches from outside sources to obtain confidential government information, the Army implemented the iWATCH Initiative.

iWATCH is a national campaign designed to increase awareness and understanding of indicators of potential terrorism or terrorism-related crimes.

The slogan for the initiative is: “If You See Something, Say Something™”
Facts About the iWatch Initiative

• iWATCH was first developed by the Los Angeles Police Department as a means of encouraging citizens to engage in safe-guarding their community

• iWATCH was first revealed in October 2009 by Los Angeles Police Chief William Bratton

As Bratton stated, “[iWATCH] is intended to be the next evolution of keeping America safe.”
Activities to Report – Use Your Senses

To help simplify the reporting process, the following guidelines were developed:

If it does not **LOOK** right, report it

If it does not **SMELL** right, report it

If it does not **SOUND** right, report it

Citizens are encouraged to report activities they deem to be suspicious and let the proper authorities determine if a terrorism-related threat exists. Citizen are not expected to be experts in identifying terrorism, nor are they expected to handle the situation themselves – leave that to the trained experts.
Examples of Suspicious Activities

• Unfamiliar individuals sketching or taking picture of specific building layouts
• Unfamiliar individuals asking in-depth questions related to security forces and/or operations
• Packages or other unfamiliar items left unattended in buildings and/or vehicles
• Unattended vehicles parked in locations typically unoccupied by motorized vehicles
• Unauthorized personnel in restricted areas
• Chemical smells or visible powders left in areas
• An unfamiliar individual asking in-depth questions about building blueprints, where specific items are stored or schedules for invited guests

While this list is not inclusive of all suspicious activities and/or behaviors, it does highlight some of the more common items which warrant reporting to the proper officials.
The more information and details you can provide the reporting officials, the more likely they will be able to intervene effectively. Some of the information you should try to provide includes:

- The date and time of the observed activity/behavior
- The location of the observed activity/behavior
- The actions/behaviors you observed by the individual(s)
- An overall description of the individual(s):
  - Gender
  - Height
  - Weight
  - Hair and skin color
  - Approximate age
- Description of their vehicle (make and model, color and license plate number)
While terrorism-related attacks can happen at any time and in any location, the following areas and facilities are the most commonly targeted:

- Joint Forces Headquarters (JFHQ)
- Installation/Base security check points
- Barracks and other lodging facilities
- Commissaries, PXs and other regularly populated facilities
- Sporting and entertainment venues
- Recreational facilities/centers
- Schools, libraries and child care centers
- Hospitals and other care facilities
- Various modes of public transportation
- Areas with large gatherings of people
Making A Report

Each installation/base and public facility will have standard operating procedures established which detail the proper steps for making a report of suspicious activities/behaviors. If you are unfamiliar with those procedures, complete the following steps:

1. Immediately contact the security and/or military police dispatch for the installation/base where you are located

2. Call the local law enforcement agency and explain the situation – they can provide additional guidance over the phone until personnel arrives

3. If it is an emergency, immediately call 911 and then work to ensure the safety of those around you/entrusted to you
OPSEC
OPERATIONS SECURITY
What is OPSEC?

OPSEC is defined as...

...a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.
What purpose does OPSEC serve?

In an ever-changing world of technology, where more and more individuals exchange information via digital systems, potential access points by criminals/hackers working to obtain confidential information become increasingly prevalent.

As contractors working in a government facility, and handling personal information on Service Members and their families, it is our responsibility to ensure all actions are taken to protect and safeguard that information.

We must always err on the side of being overly cautious and protective of all information entrusted to us or that we have access to.
Digital/Cyber Attacks

The statistics surrounding the occurrence of digital/cyber attacks are staggering. The CNN news network released the following statistics:

- Nearly 1 million new malware threats are released each day, all designed to gain access to personal information
- It is estimated 20 million cyber attacks happen each day around the world
- According to some studies, it is estimated 5,000 cyber attacks happen each hour in the United States

Remaining diligent in our efforts to protect information is critical in the government setting.
Digital/Cyber Attacks

The statistics surrounding the occurrence of digital/cyber attacks are staggering. The CNN news network released the following statistics:

- Nearly 1 million new malware threats are released each day, all designed to gain access to personal information.
- It is estimated 20 million cyber attacks happen each day around the world.
- According to some studies, it is estimated 5,000 cyber attacks happen each hour in the United States.

Remaining diligent in our efforts to protect information is critical in the government setting.
In a statement recently released from former CIA Director, George Tenet...

“The number of known adversaries conducting research on information attacks is increasing rapidly and includes intelligence services, criminals, industrial competitors, hackers and aggravated and/or disloyal insiders.”
When learning about or talking to individuals about OPSEC, you may hear the phrase “OPSEC Indicator” being used.

What is an OPSEC Indicator?

At its core, an OPSEC Indicator is a piece of information hackers or terrorism-related entities can exploit to gain access to personal and confidential information on Service Members, family members, business and organizations (like the National Guard, Army and Department of Defense).
The 5 Steps of OPSEC

Determining critical information, and then protecting that information, is the core of OPSEC. The following steps can help you to better ensure the security of information within your possession:

Step 1: Determine What is Critical Information
Step 2: Identify Potential Threats
Step 3: Identify Points of Vulnerability
Step 4: Determine Potential Risks
Step 5: Identify Possible Countermeasures
The 5 Steps of OPSEC

**Step 1: Determine What is Critical Information** – This would include any documents, recordings and/or videos containing personal information on individuals, businesses, organizations and missions (first and last names, dates of birth, addresses, banking/routing numbers, phone numbers, dates of travel, etc.).

To be safe... Consider all information you have access to to be critical information requiring necessary measures to keep it secured!

**Step 2: Identify Potential Threats** – Email phishing and spam messages, competitors, former/terminated staff members, volunteers, disgruntled employees, foreign governments/agencies – any individual is capable of divulging critical information
The 5 Steps of OPSEC

**Step 3: Identify Points of Vulnerability** – This would include potential weaknesses in relaying information, inappropriate use of email/attachments, not being aware of how to encrypt or protect information, poor oversight and management of information or even the blatant disregard for established safety measures and procedures

**Step 4: Determine Potential Risks** – Should information make its way into the wrong hands, what would the resulting risks be? Access to secured information, bank accounts, addresses and homes, program missions and timelines, dates of important events/travel... One small oversight in securing information can have drastic and wide-spread negative impacts on individuals, businesses, organizations and the military
The 5 Steps of OPSEC

Step 5: Identify Possible Countermeasures – Should information make its way into the hands of a cyber attacker or other potentially harmful entity, immediately notify your direct supervisor, State Family Program Director and security offices...

Be proactive and avoid discussing confidential/personal information in public areas like conference rooms, hallways, restrooms or other common areas, encrypt emails when possible, when transporting printed/hardcopy materials... use envelopes and folders, never leave information lying around in your workspace... cover it or file it away safely

Remember... Every operation has its own set of vulnerabilities, our job is to properly address those and ensure we are complying with established policies and procedures
INFORMATION SECURITY AWARENESS
Classified Information

While your access to ‘classified’ information as a Child and Youth Program Coordinator will most likely be very limited, should you find yourself handling information deemed as ‘classified,’ remember the following:

- Never leave classified information unattended
- Never discuss classified information in public areas
- Use of secured telephone lines and fax lines must be utilized when transferring classified information
- Classified information must remain under the control of the trusted individual
- Never stored in unsecured/unlocked spaces
- Never be stored or transferred on your computer unless proper approval has been granted by the government
Again, while your access to classified information may be minimal, it is important to have an awareness of the types of information often deemed as ‘classified’ by the government:

- Military plans, weapon information/storage and missions
- Intelligence activities, sources and agencies
- Scientific, technical and economic matters related to national security and defense
- U.S. Government plans for upcoming missions, operations or facilities
- Identified vulnerabilities or capabilities of individual systems, infrastructure, projects or services related to national security and defense

This is a partial list of the most common types of classified information; however, there are many more and these lists often change with the development of new systems, missions and operations.
Levels of Classification of Information

The U.S. classification of information system has three classification levels...

**TOP SECRET:** This level of classification is given to information which, upon disclosure, could reasonably cause exceptionally grave damage to national security

**SECRET:** This level of classification is given to information which, upon disclosure, could cause serious damage to national security

**CONFIDENTIAL:** This level of classification is given to information which, upon disclosure, could result in damage to national security

While the majority of information you have access to as a Child and Youth Program Coordinator will not fall into one of these three classification levels, you must still handle all information with the strictest of security and confidentiality to protect all individuals.
Maintaining Confidential Information

As a company, Cognitive will ensure any and all information on employees, contracts and other Child and Youth Program information is secured and safe-guarded at all times.

As contractors in the government setting, you must abide by the established policies, procedures and protocols set forth by the government. This includes, but is not limited to...

- Ensuring all work-related information is transferred via contract/gov’t-issued equipment (computers, laptops, office and cell phones)
- Maintaining possession of your CAC and building cards/keys at all times
- Using only gov’t approve storage devices which have been guaranteed to be virus-free
- Old or outdated information is shredded and disposed of properly
Information Security Violation Disciplinary Actions

**Security Infraction**: occurs when information is not safeguarded appropriately but does not result in operations being compromised

**Security Violation**: occurs when information is not safeguarded appropriately and the probability of operations being compromised is likely to occur

**Security Compromise**: occurs when information has not been safeguarded appropriately, resulting in negative impacts to operations and security

**Disciplinary actions for MINOR violations may include:**
- Verbal counseling by employer
- Written counseling by employer
- Suspension or termination by employer

**Disciplinary actions for MAJOR violations may include:**
- Imprisonment and/or fines
- Any action applicable to minor violations
- Loss of security clearance and government access cards
- Arrest
Information Security Contacts

As a contractor, should you suspect personal/classified information has been compromised, take the following action:

- Contact your immediate supervisor as well as your government point of contact (SFPD)
- Report the information to your state/territory’s security office
- Contact the Defense Hotline: 800-424-9098 (toll-free), 703-604-8799 (commercial) or 664-8799 (DSN)

Remember... Our job is to ensure the safety and security of our military Service Members, families and youth, whether working with them in-person or handling personal information. As a Child and Youth Program, contractor and team, we are only as strong as our weakest link...

Take all measures necessary to protect those we serve!
As evidence of completion of this course, you will need to complete the short assessment tool provided. To access the assessment, please click on the link below:

CLICK HERE TO BEGIN YOUR ASSESSMENT:

https://www.classmarker.com/online-test/start/?quiz=tmr574746cc5a42a

Please Note: Following completion of the assessment, please email the results certificate to your RAPM. This will serve as your documentation of completion.
You have now completed the iWatch, OPSEC and Information Security Awareness module. Congratulations!