



# REPORTING ADVERSE INFORMATION

under the Continuous Evaluation Program (CEP)

Protecting Classified Information is Everyone's Business



# Continuous Evaluation Program (CEP)

CEP Defined:

*Once an employee has been granted access to classified information, the employee falls under the CEP as long as access to classified information is contractually required. CEP involves the uninterrupted assessment of an individual in order to retain a security clearance. It includes reinvestigation at given intervals based on the level of access to classified information as well as the reporting of adverse information.*



# Continuous Evaluation Program (cont.)

Information from the following sources is reviewed as part of the CEP:

## 1. The reinvestigation process (SF 86)

- Top Secret (5 years)
- Secret (10 years)

## 2. Reporting Requirements:

- Status Changes (name, citizenship)
- Foreign Travel
- Continuing Contact with Foreign Nationals
- Suspicious Contacts
- Espionage, Sabotage, Terrorism or Subversive Activities
- Loss, Compromise or Suspected Compromise of Classified Information
- Security Violations
- Security Infractions
- Adverse Information (the focus of today's brief)



# Continuous Evaluation Program (cont.)

Information from the following sources is reviewed as part of the CEP (cont.):

## 3. Local Information Sources:

- Personnel files, medical files, security, law enforcement & intelligence files, alcohol & drug abuse program files, and special security program files

## 4. Federal Agency Information Sources:

- FBI, CIA, DOD Criminal Investigative Agencies, financial information, citizenship information

## 5. Other sources of Information:

- Local agencies where the subject has lived, worked, or attended school
- Media sources, private citizens, government employees, and work associates



# Adverse Information

If you aren't really sure what adverse information is, here's a definition:



*“Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security”*



# A Few Facts...

just so you know...



Fact #1: Life can be hard.

Sometimes we make bad decisions, act stupidly, or stuff happens to us over which we have no control.

That doesn't make us bad people, just human.



just so you know...

Fact #2: When human frailty puts a person in a bad place it needs to be reported to ensure that the actions of the person don't end up making them a risk to national security.

*“If every instinct you have is wrong, then the opposite would have to be right.” –Jerry Seinfeld*

Few people set out to betray their country, but one bad decision can lead to another, and before you know it you're living a life the exact opposite of what you thought it would be. The only way to counter a bad decision, a stupid act, or uncontrollable circumstances is to do the right thing. Reporting the negative can lead to a positive outcome because not only is it required, it's the right thing to do.



just so you know...

**Fact #3:** There is nothing wrong with disagreeing with the laws or policies of our country. However, the methods used to make desired changes determines whether someone is a security risk. People who want to change or implement laws or national policies using illegal means are a security risk. They aren't going to report their activities, so it's up to others to report what they know.

One incident of wrongdoing may be nothing, but if never reported, a pattern can't be discerned to determine a threat and possibly counter adversarial acts.

**Fact #4:** Rumor or innuendo is not to be reported. NO gossip. NO vengeance. Only what you KNOW.





just so you know...

**Fact #5:** Reporting adverse information on someone else is not an accusation, it's merely stating the facts as you know them. Determining the threat of those facts is the job of adjudicators.

**Fact #6:** Reporting adverse information is not being a tattletale. It's required if you hold a security clearance; so reporting adverse information is indirectly a part of your job description.

**Fact #7:** Adverse information does not necessarily result in the loss of a security clearance. Once reported, the facts surrounding the incident are investigated and reviewed, and a determination is made using adjudicative guidelines, taking into consideration any mitigating circumstances.



# Silver Lining

If they gave security clearances only to people with perfect lives, none of us would have one. Determinations are based on the “whole person” concept, so what you did...when you did it...what you’re doing to fix it...are some of the details taken into account.

Adjudicators are looking for trustworthiness and reliability. Not withholding information, following the rules and working to fix your issues are evidence of those qualities.

It would be great if everyone self-reported, but since none of us really know who others are, reporting adverse information about someone else is one of the means by which classified information may be protected.



# Why You Should Report Adverse Information...

## Reporting Adverse Information:

- 1) Protects our country by protecting classified information
- 2) Protects our company by protecting our facility clearance and our contracts
- 3) Protects the person whom you report by possibly thwarting a threat
- 4) Helps the person whom you report by providing intervention to negative or destructive behavior
- 5) Protects you (and your job) by doing what's required of you



Below are a list of areas that could reflect adverse information in a person's life (the following frames detail specific information that should be reported under each of these categories):

- A. Allegiance to the United States
- B. Foreign Influence
- C. Foreign Preference
- D. Sexual Behavior
- E. Personal Conduct
- F. Financial Considerations
- G. Alcohol Consumption
- H. Drug Involvement
- I. Psychological Conditions
- J. Criminal Conduct
- K. Handling Protected Information
- L. Outside Activities
- M. Use of Information Technology (IT) Systems



# Allegiance to the United States

## REPORT

(only known activities of the following nature)

- Sabotage of government or company property or facilities
- Providing classified information to another country
- Treason by acts of war against the U.S. or aiding those who wage war
- Violent acts or threatening violent acts intended to bring change
- Attempts to overthrow the U.S. government or attempting to persuade others to do likewise
- Association or sympathetic to persons committing above acts



# Foreign Influence

*Foreign influence* is about a person's vulnerability to coercion, exploitation or pressure from foreign connections whereas *foreign preference* (*next frame*) is an individual's partiality to a foreign country over the U.S.

## REPORT

(only known activities of the following nature)

- Immediate family member or close association with a person with close ties to a foreign government
- Failure to report close association with a foreign national
- Unauthorized association with a member from a foreign intelligence service
- Sharing living quarters with a foreign national
- Conduct that might bring a person to the attention of foreign officials (e.g., violation of foreign laws, frequent contact with foreign nationals, violation of customs, moral values or religious practices)
- Substantial financial interest in a country or foreign owned business



# Foreign Preference

*Foreign preference* is an individual's partiality to a foreign country over the U.S. whereas *foreign influence (previous frame)* is about a person's vulnerability to coercion, exploitation or pressure from foreign connections

## REPORT

(only known activities of the following nature)

- Dual citizenship
- Possession or use of a foreign passport
- Foreign military service
- Accepting benefits from a foreign country
- Establishing residence in a foreign country to meet citizenship requirements
- Using foreign citizenship to protect financial interests
- Seeking/holding foreign office
- Voting in foreign elections
- Acting to serve the interests of a foreign government



# Sexual Behavior

## REPORT

(only known activities of the following nature)

- Behavior involving an illegal act (e.g., prostitution, sex with a minor) regardless of prosecution or conviction
- Compulsive, self-destructive or high risk behavior that could indicate a personality disorder (e.g., uncontrolled sexual impulses)
- Behavior that could subject an individual to blackmail
- Behavior that reflects a lack of judgment (e.g., sexual harassment, sex in the workplace)





# Personal Conduct

Relates to two general categories – dishonesty or lack of candor during the personnel security process – and other conduct that raises questions about an individual's trustworthiness

## REPORT

(only known activities of the following nature)

- Omission or falsification of facts on documents
- Unwillingness to comply with rules and regulations
- Association with persons involved in criminal activity
- False or misleading information provided to officials
- Credible adverse information not explicitly covered under any other guideline related to the following:
  - Untrustworthy or unreliable behavior
  - Disruptive, violent or otherwise inappropriate behavior in the workplace
  - A pattern of dishonesty or rule violations
  - Evidence of significant misuse of employer's time or resources



# Financial Considerations

## REPORT

(only known activities of the following nature)

- Unexplained affluence
- Spending beyond one's means
- Debts caused by frivolous or irresponsible spending and the absence of intent to repay
- Consistent spending beyond one's means
- Failure to file or fraudulent filing of income taxes
- Compulsive or addictive gambling
- Inability or unwillingness to satisfy debts
- History of not meeting financial obligations
- Deceptive or illegal practices
- Financial problems linked to drug or alcohol abuse or other issues of security concern
- Illegal or deceptive financial behavior (e.g., embezzlement, check fraud)



# Alcohol Consumption

## REPORT

(only known activities of the following nature)

- Alcohol-related incidents away from work (e.g., DUI, fighting, domestic abuse)
- Alcohol-related incidents at work (e.g., drinking on the job, reporting for work impaired)
- Habitual or binge consumption
- Diagnosis of alcohol abuse or dependence without following a treatment plan, or relapse following treatment
- Failure to follow court-ordered treatment



# Drug Involvement

## REPORT

(only known activities of the following nature)

- Drug abuse (i.e., use of an illegal drug or use of a legal drug in a manner that deviates from approved direction)
- Testing positive for illegal drugs
- Illegal activities involving drugs (possession, cultivation, purchase, sale, distribution, possession of drug paraphernalia)
- Diagnosis of drug abuse or drug dependence
- Failure to successfully complete a drug treatment program
- Express intent to continue illegal drug abuse, or a failure to clearly and convincingly commit to discontinuing use



# Psychological Conditions

## REPORT

(only known activities of the following nature)

- Behavior that casts doubt on an individual's judgment, reliability, or trustworthiness not covered under a different guideline (e.g., emotionally unstable, irresponsible, dysfunctional, violent, paranoid or bizarre behaviors)
- A qualified mental health professional's opinion that a condition can impair an individual's judgment, reliability or trustworthiness
- An individual's failure to follow treatment advice related to a diagnosed psychological condition (e.g., take prescribed medication)



# Criminal Conduct

## REPORT

(only known activities of the following nature)

- A serious crime or multiple lesser offenses
- Dishonorable discharge from the Armed Forces
- Allegation or admission of criminal conduct, whether or not charged, prosecuted or convicted
- Currently on parole or probation
- Violation of parole or probation



# Handling Protected Information

## REPORT

(only known activities of the following nature)

- Deliberate or negligent disclosure of classified information
- Storing or handling classified information in an unauthorized manner
- Attempting to access classified or personally identifiable information without a need-to-know
- Attempting to remove or conceal classified markings
- Viewing information on a secure server beyond one's need-to-know
- Failure to comply with rules and regulations for protecting classified information
- Negligent security habits even after proper training and counseling



# Outside Activities

## REPORT

(only known activities of the following nature)

- Employment or service, whether compensated or voluntary, with the following entities:
  - Government of a foreign country
  - Any foreign national organization or other entity
  - A representative of any foreign interest
  - Any foreign, domestic or international organization engaged in analysis, discussion or publication of material on intelligence, defense, foreign affairs or protected technology
  - Failure to report or fully disclose an outside activity, when required





# Use of Information Technology (IT) Systems

## REPORT

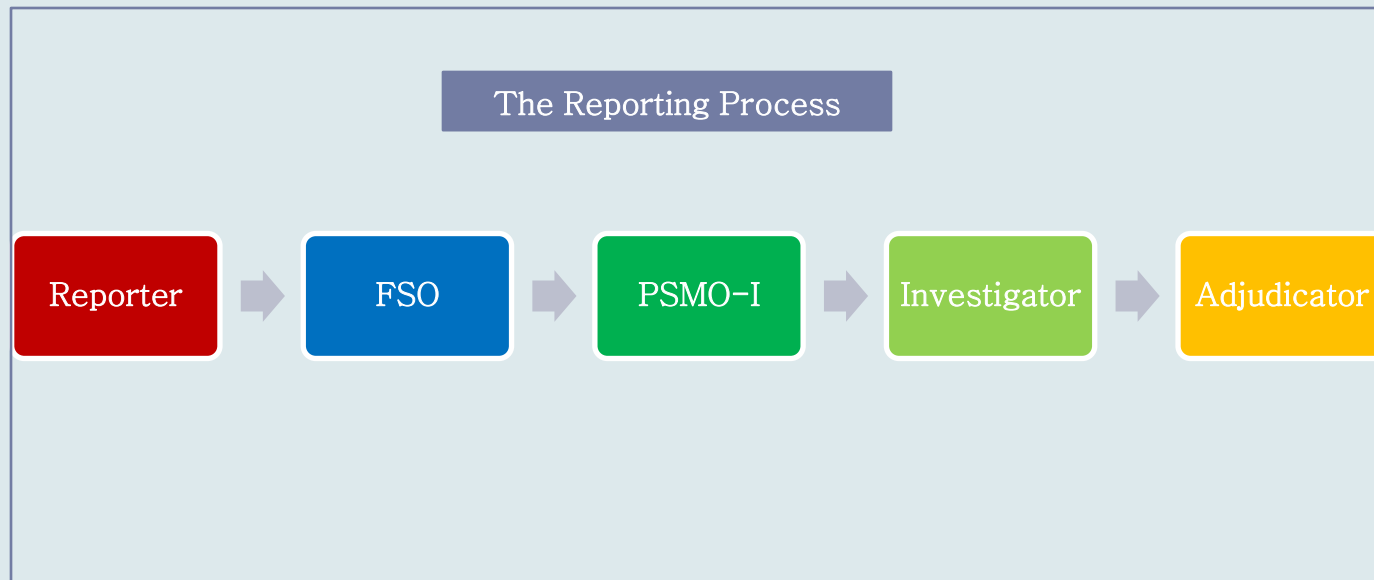
(only known activities of the following nature)

- Illegal or unauthorized entry into, modification or manipulation of, destruction or denial of access to, or removal or duplication of hardware, firmware, software, or media from any IT system
- Use of IT systems to gain unauthorized access to another system or to a compartmented area within the same system
- Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or IT system
- Misuse of IT, whether deliberate or negligent, that results in damage to national security



# To Whom do you Report?

Report adverse information to the RED-INC FSO



*Your privacy and your integrity will be respected.*



## Conclusion...When it is and isn't Everyone's Business

Many people think reporting adverse information is like getting in someone else's business. But protecting classified information is everyone's business, especially those who hold security clearances...and it isn't about only those you work with; self-reporting is required, also.

There are few secrets in our world today, so not reporting your own stuff just adds to any problem because it gives the appearance that you're trying to hide something.

Reporting is confidential and information provided is not shared within the company unless there is evidence that company policy is being violated or someone is a danger to themselves or others.

If the reporting results in a loss of access to classified information where it is required to work the contract, management and the appropriate government officials will be notified of the loss of access.



To confidentially report adverse information  
contact the RED-INC Facility Security Officer

Valerie James:

[valerie.james@red-inc.us](mailto:valerie.james@red-inc.us)

301-737-4361 ext. 23

