



U.S. DEPARTMENT OF  
**ENERGY**

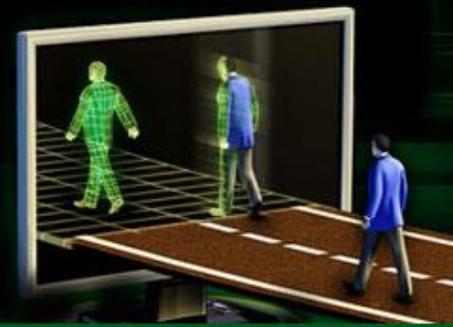
# A Matter of Trust

The Insider  
Threat  
Revealed



**Office of Environmental Management (EM)**  
*safety • performance • cleanup • closure*

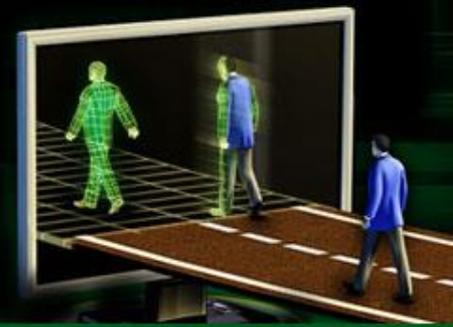
# Agenda



This training is designed to help EM personnel to recognize and identify insider threat indicators and to escalate those concerns to the proper channels.

- Understanding the Insider Threat
- Indicators for Identifying Insider Threat
- Risk Management of Insider Threat
- Insider Threat Reporting
- Q&A

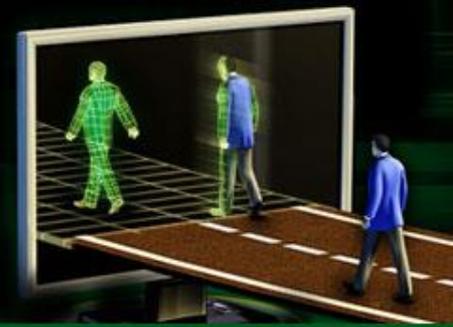
# Understanding the Insider Threat



An **Insider threat** is a malicious threat to an organization that comes from individuals within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.



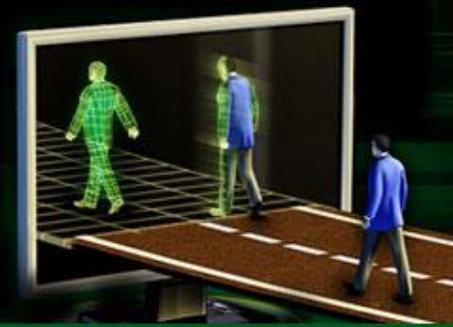
# Understanding the Insider Threat



**Insider:** Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems



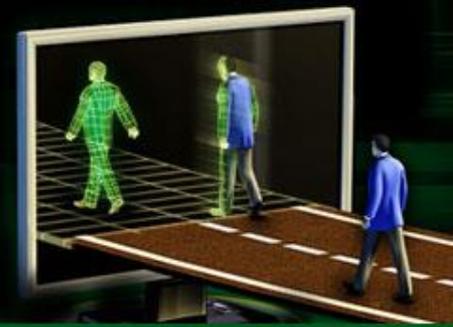
# Understanding the Insider Threat



**Insider Threat:** The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or degradation of U.S. Government resources or capabilities.



# The Insider Threat



## Malicious

- Administrators
- Privileged Users
- Super Users



## Exploited Insiders

- Users tricked into providing sensitive data
- Social Engineering
- Poor Security Habits



## Careless Insiders

- Delete Information
- Modify Information
- Poor Security Habits

# The Insider Threat



## The Era of Big Data

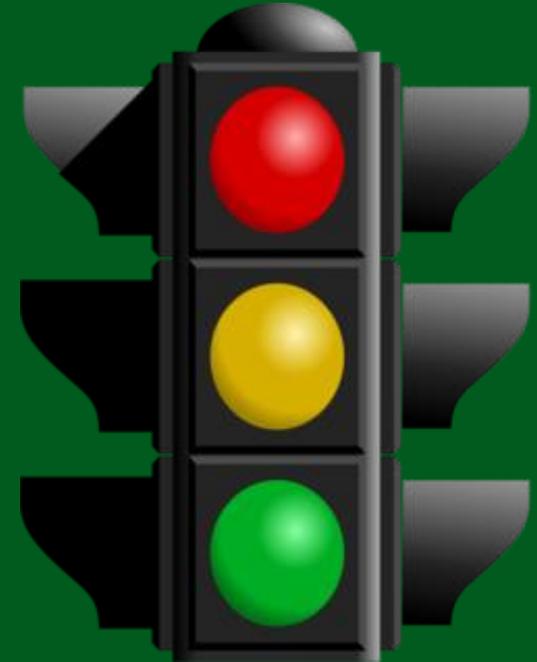
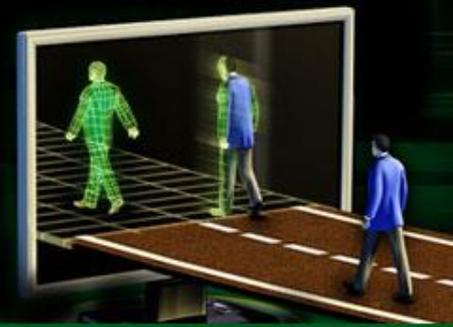
### The Rise of Big Data Analytics

- Storage of vast quantities of data to uncover patterns and insights
- In some cases, highly sensitive data
  - Personal Information
  - Credit Cards
  - Transactions
  - Communications
  - Locations

Insider Target

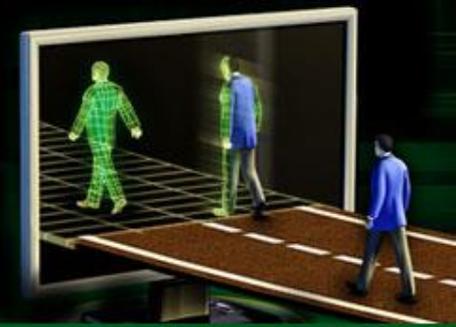


# Insider Threat Indicators



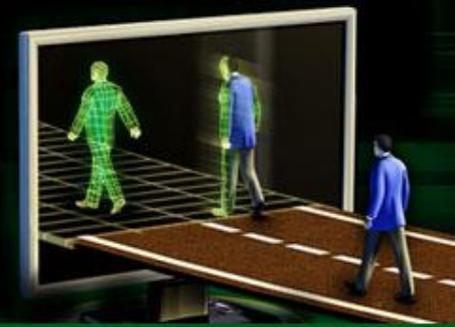
- Abnormal mood swings or depression, withdrawn behavior, decrease in hygiene, paranoia
- Flashbacks to prior traumatic events
- Abuse of alcohol or drugs
- Repeat violation of established policies
- Talk of domestic or financial problems
- Talk of suicide
- Anti-Organizational statements
- Aggression or threats towards co-workers
- Attempts to communicate with enemies of the United States
- Hatred toward other groups or religions

# Insider Threat Indicators



Stage	Indicators	Countermeasures
<b>Defection</b> Internal decision to act against the interests of the USA	If the potential threat is truly conflicted, this conflict will be evident in behavior. <ul style="list-style-type: none"> <li>• Research; visits to questionable websites</li> <li>• Concealed communications.</li> <li>• Questions or arguments about loyalty.</li> <li>• Exploring other loyalties</li> </ul> The case studies above demonstrate that there is frequent internal conflict prior to defection.	Express loyalty Express concern – suggest employee assistance or other paths to reconciliation Escalate concern
<b>Plan</b> Identify data or vulnerabilities	Searching for vulnerability data beyond that which is required for the job	Follow procedures Escalate concern
<b>Prepare</b> Collect tools & exploits consolidate information	Large files Encrypted files Files outside “Need To Know” Diminished job performance as the threat actor diverts effort to betrayal	Follow Need to Know Escalate concern
<b>Execute</b> Act against the interests of the USA	Minimal indicators – if insider threat’s preparation exceeds ours, there will be no indicators.	Prepare architecture to detect & arrest exfiltration Prepare architecture to detect & inhibit malware.

# The Insider Threat Cyber Chain



## Recruitment

- Recruitment
- Going from good to bad

## Search / Recon

- Find the target/data
- Knowledgeable threat

## Acquisition / Collection

- Grab the data

## Egress / Extraction

- Game over!
- Egress of data

## Tactical Operation

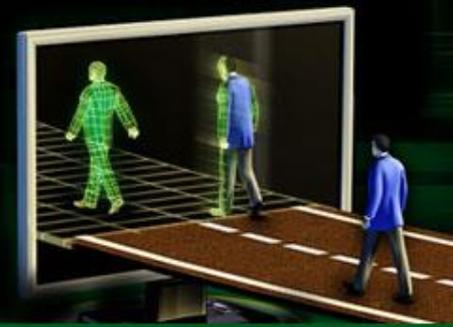
- Hiding communication with external parties

- Vague searching
- Asking coworkers to find data for them

- Use of crypto
- Renaming file extensions

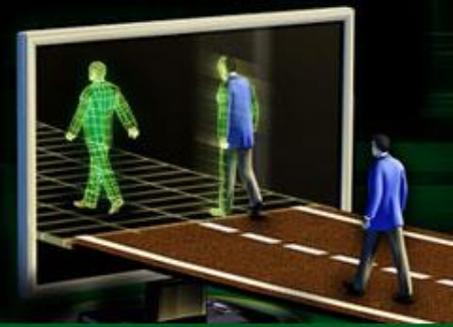
- Off hour transfers
- Spreading data downloads over multiple sessions

# Insider Risk Management



- Effective management of privileged users
- Appropriate role and entitlement assignment
- Good overall identity governance
- Proper information classification
- Good auditing and analytics
- Reducing audit log complexity
- Predictive response, not reactive
- Comprehensive Acceptable Use Policies

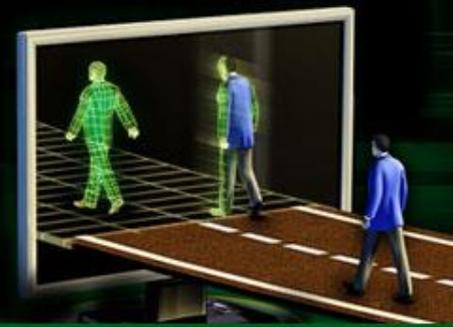
# Insider Threat Reporting



- Encourage employees to report
- Provide confidential means of reporting
- Staff holding security clearance are required to report adverse information, including potential threats
- Its better to report something that turns out to be nothing than not to report a serious security issue
- **Trust your instincts**, if you see something, say something!

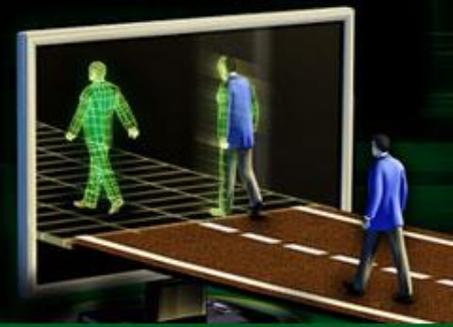


# Insider Threat Reporting



- If you suspect a present insider threat danger to your working environment, please contact your security officer
- *This slide is a place holder for future information for Field Site reporting protocols*

# Case Study Exercise

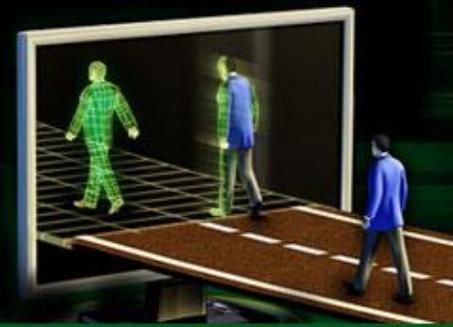


Consider the following employees and recommend one of the following three approaches:

- A) No action
- B) Act with compassion - recommend existing Employee Assistance Programs, supervisor intervention or other low conflict, high support options
- C) Escalate counterintelligence concerns through normal channels

Case 1: Employee is an average performer, but his work performance suffers before every election. He gets to work early, and leaves on time. He has always been political. He has been counselled three times for his political speech at work, Once for a heated tirade condemning the "Republicrats", once for displaying Libertarian campaign literature at work, and once for a heated argument in which he told a co-worker that he couldn't believe she was stupid enough to believe that the current administration was related to the founding fathers.

# Case Study Exercise

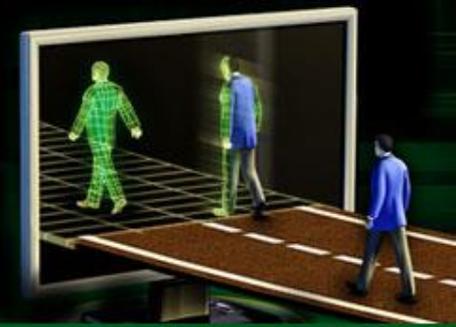


Consider the following employees and recommend one of the following three approaches:

- A) No action
- B) Act with compassion - recommend existing Employee Assistance Programs, supervisor intervention or other low conflict, high support options
- C) Escalate counterintelligence concerns through normal channels

Case 2: Employee was a high performer, but of late he has changed. He shows up for work wearing all black, and looks exhausted. He has missed deadlines and turned in low quality product that required rework. He is distracted and unengaged.

# Case Study Exercise

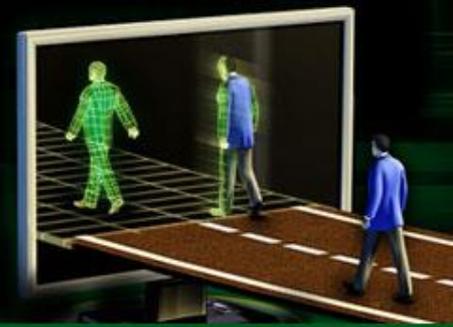


Consider the following employees and recommend one of the following three approaches:

- A) No action
- B) Act with compassion - recommend existing Employee Assistance Programs, supervisor intervention or other low conflict, high support options
- C) Escalate counterintelligence concerns through normal channels

Case 3: Employee is an average performer whose performance has dropped. He is clearly distracted and hiding something - several co-workers have commented that he has rushed to hide something on his screen when they've walked into his office. They can't put their fingers on exactly what, but he is no longer the friendly person he once was; he is withdrawn and solitary.

# Case Study Exercise

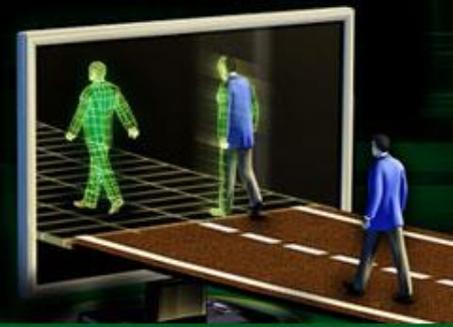


Consider the following employees and recommend one of the following three approaches:

- A) No action
- B) Act with compassion - recommend existing Employee Assistance Programs, supervisor intervention or other low conflict, high support options
- C) Escalate counterintelligence concerns through normal channels

Case 2: Employee is an average performer. He is deeply religious; at lunch or on breaks he withdraws to pray or to read religious texts. He politely declines to eat with or socialize with people who do not share his faith. He has been counseled twice for engaging in religious discussions at work; the second case was officially investigated and several co-workers testified that he was baited into the discussion - that he had done everything he could to avoid the topic, but the co-worker in question verbally attacked core tenets of Mark's belief. In the past week, there has been a public scandal involving members of his religion; Although Mark is clearly affected, Mark has politely rebuffed co-workers expressions of sympathy and interest and declined to comment.

# Case Study Exercise



Consider the following employees and recommend one of the following three approaches:

- A) No action
- B) Act with compassion - recommend existing Employee Assistance Programs, supervisor intervention or other low conflict, high support options
- C) Escalate counterintelligence concerns through normal channels

Case 2: Employee is an average performer. Recently he has volunteered to work on several projects that extend his abilities and applied for after hours training in economics to extend his abilities further and give him more opportunities. He has always been an enthusiastic reader, but has become fascinated by Thomas Piketty and the 99% movement. His co-workers joke that he can explain the world series results through reference to Piketty.

# Q&A

