

# **Information Assurance Fundamentals**

---

## **Situational Awareness Tips**

### **To avoid being targeted by adversaries:**

- Remove your security badge after leaving your workstation
- Don't talk about work outside your workspace unless it is a specifically designated public meeting environment and is controlled by the event planners
- Even inside a closed work environment, be careful when discussing classified or sensitive information, such as PII or PHI, as people without a need-to-know may be present
- Avoid activities that may compromise situational awareness
- Be aware of people eavesdropping when retrieving messages from smartphones or other media

## **Social Engineering Tips**

Social engineers use telephone surveys, e-mail messages, Websites, text messages, automated phone calls, and in-person interviews.

### **To protect against social engineering:**

- Do not participate in telephone surveys
- Do not give out personal information
- Do not give out computer or network information
- Do not follow instructions from unverified personnel
- Document interaction:
  - Verify the identity of all individuals
  - Write down phone number
  - Take detailed notes
- Contact your security POC or help desk
- Report cultivation contacts by foreign nationals

## Insider Threat Tips

An insider threat uses authorized access, wittingly or unwittingly, to harm national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

Insiders are able to do extraordinary damage to their organizations by exploiting their trusted status and authorized access to government information systems.

In one report on known U.S. spies from 1947 to 2001, these individuals:

- Demonstrated behaviors of security concerns: 80% of the time
- Experienced a life crisis: 25% of the time
- Volunteered: 70% of the time

***Although the vast majority of people are loyal and patriotic, the insider threat is real and we must be vigilant in our efforts to thwart it.***

To protect against the insider threat, be alert to and report any suspicious activity or behavior or potential security incident in accordance with your agency's Insider Threat policy:

- Attempt to access sensitive information without the need-to-know
- Unauthorized removal of sensitive information
- Unusual request for sensitive information
- Bringing an electronic device into prohibited areas
- Sudden purchases of high value items/living beyond their means
- Overseas trips for no apparent reason or of short duration
- Alcohol or drug problems

## Potential Insider Threat Indicators

How do we defend against these individuals? By using our powers of observation to recognize ***potential*** insider threat indicators, such as:

- Difficult life circumstances
  - Divorce or death of spouse
  - Alcohol or other substance abuse or dependence
  - Untreated mental health issues

- Financial difficulties
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Unexplained or sudden affluence
- Unreported foreign contact and travel
- Inappropriate, unusual, or excessive interest in sensitive or classified information
- Mishandling of classified information
- Divided loyalty or allegiance to the U.S.

Individuals experiencing stressful situations may be vulnerable to exploitation.

## **Identity Theft Tips**

Social engineering can result not only in the disclosure of sensitive government information, but also in identity theft.

### **To protect your identity:**

- Ask how information will be used before giving it out
- Pay attention to credit card and bank statements
- Avoid common names or dates for passwords and PINs
- Pick up mail promptly
- Shred personal documents
- Refrain from carrying SSN card and passport
- Order credit report annually

### **To respond to identity theft if it occurs:**

- Contact credit reporting agencies
- Contact financial institutions to cancel accounts
- Monitor credit card statements for unauthorized purchases
- Report crime to the local law enforcement

## **Tips for Teleworking**

- Obtain permission from your organization
- Follow your organization's guidance to telework
- Use authorized equipment and software and follow your organization's policies
- Perform telework in a dedicated area at home
- Don't remove classified documents from your workspace