

## Cyber Awareness Challenge Reference Material

# 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

Insider Threats are threats from people who have access to the organization's information systems and may cause loss of physical inventory, data, and other security risks.

#### To protect against the insider threat:

- Be alert to and report any suspicious activity or behavior
- Be alert to and report potential security incidents

## 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