DOD-US1364-21 Cyber Awareness Challenge 2023-2024 Complete Solutions

Spillage: how should you respond if you receive an inquiry for info not clear for public release? - Refer your order to PAO.

Spillage: what will help prevent spillage? - Follow procedures for transfering data to and from outside agency and networks.

Classified data: what is the basis for handling classified data? - Classification level and handling caveats

Classified data: who designates classified data? - Original Classification Authority

Insider Threat: which is the following of a potential insider threat? - Difficult life circumstances

Insider threat: what function do insider threat programs aim to fulfill? - Proactively identify future threats and formulate wholistic mitigation responses

Insider threats: what is a reportable insider threat? - A colleague removes sensitive info w/o seeking authorization in order to perform authorized telework

Social Networking: when might you be subject to criminal, disciplinary, or administrative action due to online harassment, bullying, stalking, etc? - If you participate/condone it in anyway

Social Networking: which of the following is a security best practice when using social networking sites? - Avoid posting pii (mothers maiden name)

Social Networking: Protect yourself on social networking sites? - Delete posts containing Personal information on a regular basis

Controlled Unclass Info: which Desi marks information that does not have the potential to damage national security - Unclassified

Controlled Unclass Info: What's true for CUI? - CUI must have diseminating controls

Controlled Unclass Info: best way to transmit CUI? - Make sure recipients are clear and need to know then send via encrypted email

Physical security: which CPCON establishes a protection policy focus critical functions only - CPCON 1

Identity Management: strong password? - @rF+13gtK5!

Identify Management: whats true about CACs? - It contains certificates for ID, encryption, and digital signature

SCI: what's true of sharing info in a SCIF? - Avoid referencing derivitavely classified reports classified higher than the recipient

SCI: what's true for transmitting SCI? - Only transmit SCI if you're courier briefed for SCI

Removable media in SCIF: what's true of PEDs in a SCIF? - Only connect government-owned PEDs to the same level classification information system when authorized

Malicious Code: what's true for downloading apps? - For government devices, use approved and authorized apps only

Website use: how should you respond to theft of identity? - Contact reporting agencies, financial institutions, monitor credit card statements and report crime to law enforcement

Social engineering: how to protect from social engineering? - Verify identity of individuals

Social engineering: common indicator of phishng attempt? - Claim that you update or validate information

Social engineering: what security issue is associated with compressed URLs? - Can be used to mask malicious intent

Travel: problems w/ public wifi? - May expose information sent to theft

GFE: what is personally owned monitor you shouldn't connect to your GFE? - USB

Mobile Devices: which is a best practice for using removable media? - Avoid inserting removable media with unknown content into your computer

Mobile devices: how can you protect data on your mobile computing and portable e-devices (PEDs)? - Auto screen locking

Home Computer: best practice for securing home computer? - Install system security patches

*Spillage
After reading an online story about a new security project being developed on the military installation where you work, your neighbor asks you to comment about the article. You know this project is classified. What should be your response? - Attempt to