EIDWS - INFORMATION ASSURANCE Cheat Sheet

by weatherman22 via cheatography.com/20977/cs/8170/

Define IA

Protecting & Defending Data

Ensuring: 1. Availability, 2. Integrity, 3. Authentication, 4. Confidentiality, 5. Non-Repudiation

Incorporating: 1. Protection, 2. Detection, 3. Reaction Capabilities

DAO

Designated Approving Authority

Configuration Management

1. Identifies, 2. Controls, 3. Accounts For, 4. Audits

In reference to a site or Information System (I.S.)

Occurs during: 1. Design, 2. Development, 3. Operational Lifecycle

9 Categories of Computer Incidents

1. Root Level Intrusion (incident)
2. User Level Intrusion (incident)
3. Unsuccessful Activity Attempt (event)
4. Denial of Service (incident)
5. Non-Compliance Activity (event)
6. Reconnaisssance (event)
7. Malicious Logic (event)
8. Investigating (event)
9. Explained Anomaly (event)

DoN WWW Security Policy

Threats to the security of Navy and Marine Corps operations

Threats to the safety of DoN personnel and their families

Attacks in the form of: 1. Computer Systems, 2. Terrorist Attacks, 3. Identity Theft

Balancing public information with OPSEC, Privacy Information, INFOSEC, and Personal Safety

NTD

Navy Telecommunications Directive

CCRI

Command Cyber Readiness Inspection

Formal inspection process which holds commanders accountable for their IA

Designated Approving Authority

Upper Level Manager

Responsible for determining Accepted Level of Risks

Determines if system meets Accreditation criteria

Cross-domain Xfer Security Procedures

Goal: Limit Risks when transferring Data

Risks: 1. Careless Methods, 2. Shortcuts, 3. Untrained Users

These risks compromise sensitive & classified information

Root Level Intrusion

Unauthorized "Privileged" access to a DoD system

User Level Intrusion

Unauthorized "Non-privileged" access to a DoD system

Example: If the system is compromised w/ malcious code that provides remote interactive control

Reconnaissance

Seeks to gather information from DoD systems, applications, networks, and users

Information can be used to formulate an attack

Does not directly result in compromise

Explained Anomaly

Suspicious events that after further investigation are deemed "non-malicious"

Deteremined to be non-malicious and don't fit any other category

IAVA

Announcement of a computer application software or operating system vulnerability notification

In the form of an alert

Service Patch

Software Package containing several updates or an App or OS

Certification

Evaluation of Technical & Non-Technical Security features of an I.S.

Incorporating: 1. Protection, 2. Detection, 3. Reaction Capabilities

5 Attributes of IA

Confidentiality

Integrity

Availability

Non-repudiation

Authentication

Integrity

Preventing information from modification by unauthorized parties or in unauthorized manners

Authentication

Assurance of the identity of a message sender or receiver

Unsuccessful Activity Attempt

Deliberate attempts to gain unauthorized access to a DoD system

Attempts are defeated by normal defensive mechanisms

Malicious Logic

Installation of software designed and/or deployed by adversaries for malicious intentions

For the purpose of gaining access to resources or information w/o consent or knowledge of the user

Alert

Information Assurance Vulnerability Alert (IAVA)

Bulletin

Information Assurance Vulnerability Bulletin (IAVB)

IAVB

Announcement of a computer application software or operating system vulnerability notification

In the form of a bulletin

Vulnerability

A known possible exploitation

Threat

A possible intrusion by a third party

Accreditation

Official Management Decision

Decision to operate an I.S. in a specified Environment

Confidentiality

Protecting information from Unauthorized Persons, Processes, or Devices

Availability

Timely, Reliable access to data and Info Systems by authorized users

Non-Repudiation

The sender of data is provided w/ Proof of Delivery

The recipient is provided w/ proof of the sender's identity

Neither can later deny having processed the data

Denial of Service

Activity that "Denies, Degrades, or Disrupts" normal functionality of system or network

Non-Compliance Activity

Activity that potentially exposes DoD systems to increased risks

Due to the the Action or Inaction of authorized users

Investigating

Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing further review

Will be re-categorized to appropriate Category 1-7 or 9 prior to closure

Computer Tasking Order (CTO)

When a computer completes all tasks assigned

Information Assurance Manager (IAM)

1. Establishing, Implementing and Maintaining the DoD IA program

2. Documenting the IA program through the DoD IA & C&A process