

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	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	IAVA Announcement of a computer application software or operating system vulnerability notification In the form of an alert	Vulnerability A known possible exploitation
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	DAO Designated Approving Authority	Root Level Intrusion Unauthorized "Privileged" access to a DoD system	IAVB Announcement of a computer application software or operating system vulnerability notification In the form of a bulletin
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. Reconnaissssance (event) 7. Malicious Logic (event) 8. Investigating (event) 9. Explained Anomaly (event)	CCRI Command Cyber Readiness Inspection Formal inspection process which holds commanders accountable for their IA	User Level Intrusion Unauthorized "Non-privileged" access to a DoD system Example: If the system is compromised w/ malicious code that provides remote interactive control	Bulletin Information Assurance Vulnerability Bulletin (IAVB)
	Designated Approving Authority Upper Level Manager Responsible for determining Accepted Level of Risks Determines if system meets Accreditation criteria	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	Alert Information Assurance Vulnerability Alert (IAVA)
	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	Explained Anomaly Suspicious events that after further investigation are deemed "non-malicious" Determined to be non-malicious and don't fit any other category	Certification Evaluation of Technical & Non-Technical Security features of an I.S. Incorporating: 1. Protection, 2. Detection, 3. Reaction Capabilities
NTD Navy Telecommunications Directive	Service Patch Software Package containing several updates or an App or OS	Threat A possible intrusion by a third party	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
			Unsuccessful Activity Attempt Deliberate attempts to gain unauthorized access to a DoD system Attempts are defeated by normal defensive mechanisms



By weatherman22

Published 10th May, 2016.
 Last updated 12th May, 2016.
 Page 1 of 2.

Sponsored by **Readable.com**
 Measure your website readability!
<https://readable.com>

Authentication

Assurance of the identity of a message sender or receiver

Integrity

Preventing information from modification by unauthorized parties or in unauthorized manners

5 Attributes of IA

Confidentiality

Integrity

Availability

Non-repudiation

Authentication

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

Computer Tasking Order (CTO)

When a computer completes all tasks assigned

Availability

Timely, Reliable access to data and Info Systems by 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

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

Non-Compliance Activity

Activity that potentially exposes DoD systems to increased risks

Due to the the Action or Inaction of authorized users

Confidentiality

Protecting information from Unauthorized Persons, Processes, or Devices

Denial of Service

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

Accreditation

Official Management Decision

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



By weatherman22

cheatography.com/weatherman22/

Published 10th May, 2016.

Last updated 12th May, 2016.

Page 2 of 2.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>