#### The Marine Corps Information Assurance Program

#### **Certification & Accreditation**

Ray A. Letteer, CISSP, NSA-IAM Chief, IA Division; USMC SIAO; USMC DAA Headquarters, US Marine Corps, C4IA



A Marine Corps fighting force armed with assured, secure, accurate, and timely information, to enhance the ability to take the fight to any enemy, anywhere, and win.



#### **Historical Perspective**

# BRINGING CIVILIZATION TO ITS KNEES .... Goths Vandals HACK HACK Incl





HACK

HACK

HACK

Ensure cyber policies, procedures, standards, and methodologies are implemented within the Marine Corps to guarantee assured information delivery, data integrity, and ensured information protection.

Marine Corps IA ensures end-to-end capability to deliver secure information at the right time, to the right place, and in a useable format, allowing commanders to exercise command and communication, regardless of proximity to their assigned forces.

## **Causes for concern**

- Poor browser configurations (XSS),
- SQL misconfigurations,
- Peer-to-peer software usage,
- Poor operating system design,
- Failure to follow policy,
- User Access Control (ID & Passwords)
- Phishing/spear-phishing email attacks increasing and becoming more sophisticated.





Motive + Means + Opportunity = ATTACK!

"As the command and control system becomes increasingly complex, it likewise becomes increasingly vulnerable to disruption, monitoring, and penetration by the enemy..." MCDP 6

#### Ingredients of an Attack



# **Cyber Security Quality Assurance**

### Certification

The <u>comprehensive evaluation</u> of the <u>technical</u> and <u>non-technical security features</u> of an information system and other safeguards, made in <u>support of the accreditation process</u>, to establish the extent to which a <u>particular design</u> and <u>implementation</u> meets a <u>specified set of security requirements</u>.

#### Accreditation

 A <u>formal</u> declaration by the DAA that an information system is <u>approved to operate</u> in a particular security mode using a prescribed set of safeguards to <u>an acceptable level of risk</u>.

### What is accredited?

 Any <u>equipment</u> or interconnected <u>system or subsystem of</u> <u>equipment</u> that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and <u>includes computer software, firmware, and hardware</u>.





# **Starting Simply**

A "Quantum Physics" primer of Information Assurance & Cyber security

- Hardware, Software, Firmware = a System
- A group of Systems = Network (sometimes called a "System of Systems")
- A group of Networks = Enclave (sometimes called a "Community of Interest")
- A group of Enclaves = Enterprise
- Software implementing services tie the hardware together.
- Consider the communication or connection protocol
- It all starts with a system that houses the data!
- Must consider the *physical* as well a *virtual!*

Keep the <u>approach</u> simple and uncomplicated

Make sure the information is <u>detailed</u> and <u>accurate</u>





### **Understanding Information**



The McCumber Cube, John McCumber, 1991



# **Documenting security progress**

- Categorizing accreditation boundary construct
  - System accreditation evaluates a major system application or a clearly defined independent system.
  - Type accreditation evaluates an application or system that is distributed to a number of different locations.
  - Site accreditation evaluates applications and systems at a specific, self-contained location.
- Determining the security control objective to meet
  - Mission Assurance Category III: baseline
  - Mission Assurance Category II: control failure kills a mission
  - Mission Assurance Category I: control failure kills a Marine







# **IA Control Inheritance**

Applications inherit IA Controls from the workstation/server on which they reside;

Workstations/Servers inherit IA Controls from the environment in which they reside



#### Examples:

COAS-1: Alternate Site Identification, Partial Mission Restoration

COBR-1: Physical Security

CODB-2: Data backup - Daily



- Adequacy of the security countermeasures selected
  - Link the control objective with the specific implementation.
  - Hint: Use the STIGs!!
  - Understand the <u>dynamic</u> nature of the threat.
- Benefits of additional countermeasures
  - Sometimes there needs to be <u>additional actions taken</u> to mitigate problems due to architecture, programmatic impacts.
- Operational needs
  - Short term support for critical, life-saving, mission actions
  - Not a free pass; still have to meet the long-term security requirements
- Available resources to reduce the risks.
  - Dollars, manpower, schedule, performance, etc.
  - Ignoring the expenditures does not remove the requirement to implement proper security!







# **Assessing the Risk**

- A security risks decisions must consider the <u>potential consequences</u>:
  - Loss of system availability due to identified vulnerabilities
  - Loss of integrity due to data alteration
  - Loss of confidentiality due to risk of disclosure
  - Loss of accountability due to authentication or non-repudiation vulnerabilities
  - Exploitation of threats in the specific system environment (i.e., combat, exercise, humanitarian relief)
- Reality of the Situation: We live in a "Risk Balanced" world
  - Risk Avoidance = so locked down, the mission can't be done
  - Risk Ignorance = so open, the mission can't be done safely
- Some risk we can accept. Some risk we can't.
  - Category 1 = unmitigated is never acceptable per DoD Directive
  - Category 2 = must be mitigated before full approval to operate (ATO) is granted



Every system/network/enclave <u>must</u> have a POA&M on the risk mitigation strategies, even with a full ATO



### **Consider the Acquisition state**



Critical to start looking at IA Controls early and build them in at the beginning



