



USA CECOM Software Engineering Center

STRATEGIES FOR SECURING TACTICAL & OFFICE INFORMATION SYSTEMS

30 April 2002



Mr. Arthur Walters
ITED Information Operations Division
DSN 992-1537
arthur.walters@mail1.monmouth.army.mil

CECOM Bottom Line: THE WARFIGHTER



CONTENTS



- **Objective**
- **Background**
- **Strategy**
- **Lessons Learned**
- **Final Comments**



OBJECTIVE

- **Objective 1 is to get everyone thinking about Information Security.**
- **Objective 2 is to present a strategy for fielding secure systems and discuss some of the pitfalls.**
- **Objective 3 is to spend all the time necessary after this presentation to answer any and all questions.**



BACKGROUND

- **Budgets are shrinking but new systems still need to be fielded and legacy systems need to be maintained.**
- **Two major tasks must be achieved:**
 - **Functionality**
 - **Security**
- **In the struggle for dollars, traditionally functionality WINS OUT.**
- **Yet if a weapon system is hacked into and an enemy re-targets the system, the results could be catastrophic!!**



BACKGROUND



- **Information Technology can be our greatest asset and also our greatest vulnerability.**
- **Intercommunication and interoperability provide increased capabilities and also allow great opportunities for exploitation by our enemies.**



DUTY



- **Our users/warfighters know what they need.**
- **It is our DUTY to use our talents, abilities and resourcefulness to get the warfighter what they need.**
- **No warfighter would accept a system which could be taken over from a remote location by the enemy.**



BUILDING A SECURE SYSTEM



Step 1 – Elicit Information Assurance help

- **Get professional information security (InfoSec) people involved early!**
- **How early? When the system's functional requirements are being developed.**



BUILDING A SECURE SYSTEM



- **Who are professional InfoSec people?**

People who do Security accreditations and Information Assurance (IA) work daily.

- **New threats and vulnerabilities arise daily. Keeping current is not a part time-job.**



BUILDING A SECURE SYSTEM, cont'd



Step 2 - Education

- **Get educated at a high level on Information Security/Information Assurance. (Get recommendations on training from your InfoSec/IA professionals.)**
- **As a part-timer you can't be up on all the latest hacker exploits or even all the tools, but you can learn enough to understand the PROCESS.**



BUILDING A SECURE SYSTEM, cont'd



THE PROCESS

- **DoD Information Technology Security Certification and Accreditation Process (DITSCAP)**
- **DoDI 5200.40 & DoD 8510.1-M**



DITSCAP



- **THE DITSCAP provides a Process and Set of Activities for accrediting all Information Systems (IS)**
- **The DITSCAP establishes a Standard process, Set of Activities, General Tasks, and a Management Structure to CERTIFY and ACCREDIT IS that will maintain the IA and Security posture of the Defense Information Infrastructure (DII).**



CERTIFICATION



- **Is the comprehensive evaluation of the technical and non-technical security features of an Information System (IS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.**

DoD (DITSCAP) Instruction 8510.1- E2.1.8.



ACCREDITATION

- **Formal declaration by a Designated Approving Authority (DAA) that an Information System (IS) is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.**

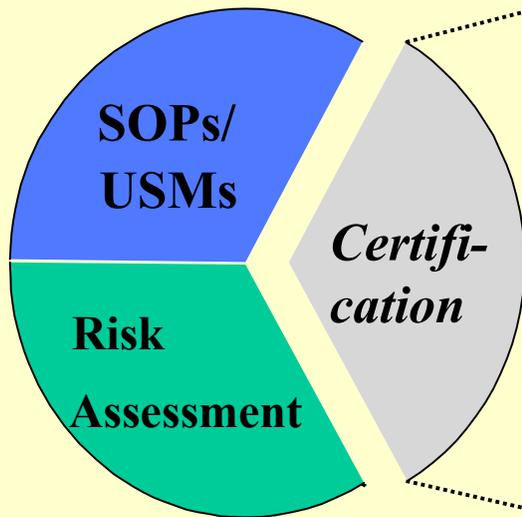
DoD (DITSCAP) Instruction 8510.1-E2.1.2.



CERTIFICATION & ACCREDITATION RELATIONSHIP

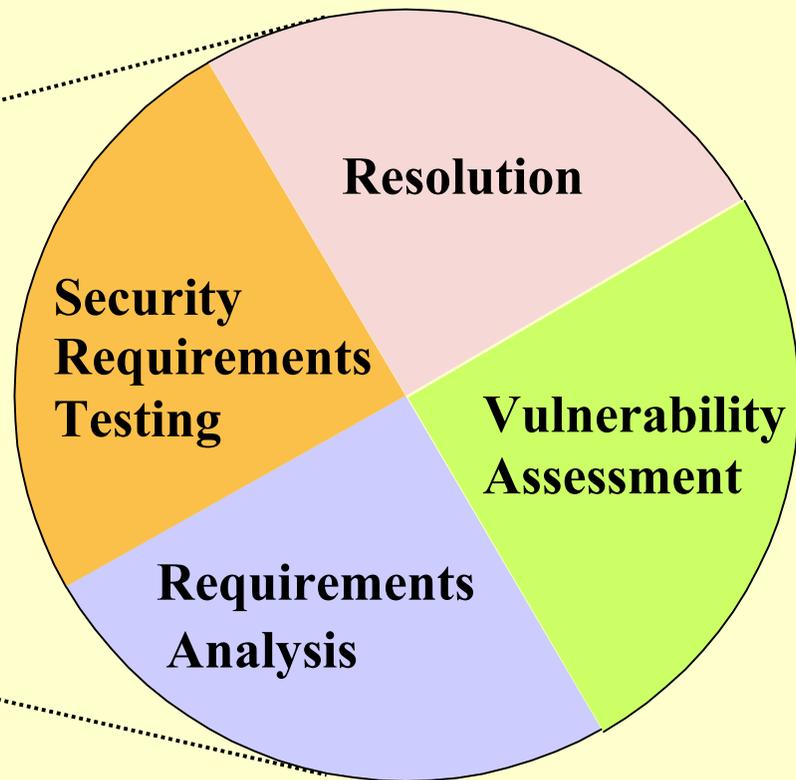


Accreditation



Standing Operating Procedure (SOP)
User Security Manual (USM)

Certification



CECOM Bottom Line: THE WARFIGHTER



ACCREDITATION

Accreditations are normally issued in one of three ways:

- (1) A System Accreditation that approves the operation of a single information system, or a network at an identified site.
- (2) A Site Accreditation that approves the operation of a defined set of information systems at an identified site.
- (3) A Type Accreditation that approves the operation of a multiple instances of an information system or s/w application.

»

(DITSCAP E3.1.3)



UNDERSTANDING RISK



Step 3 – Understanding Risk

Risk can be broken down into three components:

- Degree of difficulty to accomplish an exploit
- Likelihood of the exploit being used
- Consequences if exploit is successful



RISK MANAGEMENT PLAN



It must address a process for clearly:

- **Identifying your system**
- **Identifying the system's security requirements**
- **Verifying compliance with the requirements**
- **Planning for addressing any requirements which are not met (correct, mitigate, or accept)**



RISK MANAGEMENT PLAN, cont'd



It must also address:

- **New threats and new exploits/vulnerabilities as they develop**
- **What your organization will do if attacked (assign roles and responsibilities)**
- **How to detect an attack**
- **How to survive/minimize the effects of an attack**
- **How to recover from an attack**



MAINTENANCE

Step 4 - Maintain the security of your system/organization

- **Security & risk level are fleeting**
- **Maintenance agreements with your security professionals are essential.**
- **By having an accreditation maintenance agreement, your IA professionals will keep your documents up-to-date and assessing how new threats & vulnerabilities may affect your system.**



LESSONS LEARNED



- **There is no such thing as HACKER PROOF!**
- **Even if it were true that at the completion of your security testing, no hackers in the world could infiltrate your system, there are new techniques/exploits coming to light every day.**
- **This work is not about absolutes; it is about ASSESSING AND MANAGING RISK.**



LESSONS LEARNED, cont'd



Combining Functional testing with security testing:

- **In theory it sounds good, but in practice functional testing takes precedence.**
- **Schedule a fixed amount of time for security testing, typically at the end of functional testing. Allow for functional test over run.**



LESSONS LEARNED, cont'd



The difficult decisions:

- **Knowing when to field and when to wait**
- **When is enough enough?**



LESSONS LEARNED,cont'd



Knowing when to field:

- **Understand the need (capability & timing)**
- **Weigh the risk versus the mission need**
- **Maybe an Interim Approval To Operate is the best solution.**



LESSONS LEARNED, cont'd



Knowing when to wait:

- Understand the risk
- Weigh the risk versus the benefit
- Maybe not having a capability is better than losing it (or having it used against you) at the critical moment .



FINAL COMMENTS

The vulnerabilities are there; so far we've been lucky. We've been lucky because the individuals with the knowledge, skill and opportunity have mostly been true hackers. They are interested in expanding their knowledge, testing their skills and maybe getting a little bragging rights.



FINAL COMMENTS



- **Although a true hacker is still breaking the law, their intent is typically not malicious.**
- **Terrorists, enemy governments, criminals, and the mentally unstable are gaining the skills necessary to exploit many of our systems.**
- **As they get better so must we.**



FINAL COMMENTS, cont'd



- **Vulnerabilities such as trap doors or back doors may already exist in DoD systems.**
- **Logic bombs, hacker tool kits, and other malicious code may already have been planted.**
- **New techniques to launch attacks are being developed.**



FINAL COMMENTS, cont'd



- **To achieve total invulnerability would be cost prohibitive (probably impossible).**
- **To do nothing is inconceivable!**
- **What we must do is to make the most of the dollars we have.**

- **IA is not a paper drill or a bureaucratic hurdle AND THIS IS NOT JUST ABOUT GETTING THE C&A BOX CHECKED.**