



ISEC: The Army's Sustaining Base Full Spectrum Information Assurance Experts

Presented by: COL John Deal

Commander

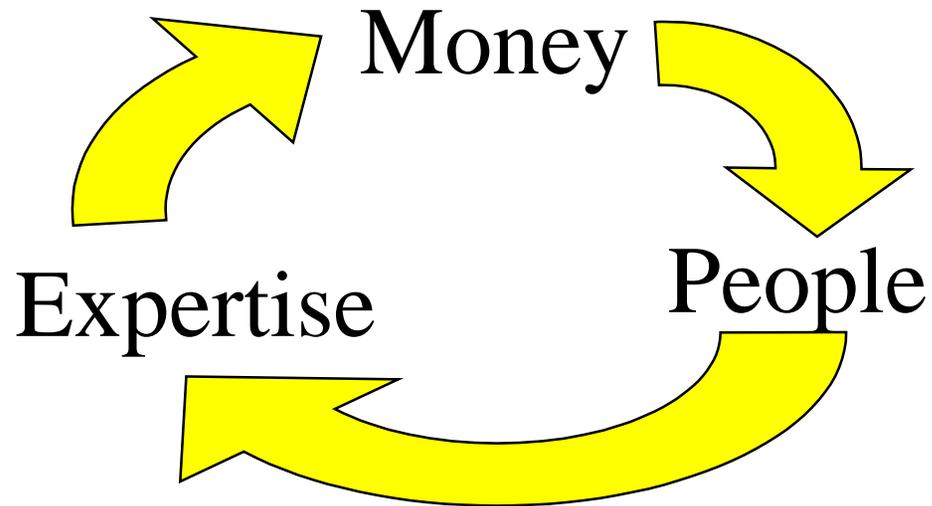
**US Army Information Systems Engineering
Command**

DSN: 879-6626

Email: dealj@hqisec.army.mil



The Information Assurance Triangle



I can't help you with money or people, but I can offer you the best Security Engineers, Certification Agents, Product Evaluators and System Engineers DoD has to offer



Some Common Terminology



- **Information Assurance is more than just C&A**
 - **Certification and Accreditation are the critical final steps in verifying and asserting a systems security posture; however,**
 - C&A provides assurance, not security
 - Security results from the thoughtful application of Security Engineering principals during a systems lifecycle
 - **Security Engineering is that specialty of Systems Engineering responsible for the identification and satisfaction of a complete systems security requirements**



IA and Systems Engineering



- **ISEC is the Army's Sustaining Base System Engineers**
 - **We bring a holistic systems approach to IA**
 - System Components
 - HW, SW, Communications, Operating Environment, Personnel, etc
 - System Lifecycle
 - From requirements to design, development, fielding, and sustainment
 - System Interaction
 - Interoperability with LAN, CAN, WAN and other systems
 - **IA is built on a solid understanding of the total system**



Full Spectrum IA



- **Because we are a System Engineering organization ISEC can provide full spectrum IA support:**
 - **Security Engineering**
 - **Product Evaluation**
 - **Modeling and Simulation**
 - **Certification Testing**
 - **Accreditation Support (DITSCAP)**
- **To the full spectrum of Army systems:**
 - **Stand Alone Servers/desktops**
 - **Multi host/server and application systems**
 - **LANs, CANs, WANs**



Security Engineering



- **Security Engineering**
 - That sub-discipline of **Systems Engineering** responsible for the identification and integration of security requirements and satisfaction of those requirements in an interdisciplinary manner throughout the lifecycle of an information system
 - Security Engineering is the heart of preparing a system to be operated and maintained securely. Everything else is associated with supporting Security Engineering:
 - Product Eval: Objective review of available tools
 - Certification: Provides assurance that the Security Engineers did their job properly in developing a secure system
 - Accreditation: Administrative statement that system is “secure enough” for it’s intended environment



Security Engineering (cont)



- **ISEC History**

- **ISEC has been incorporating Security Engineering into our customers systems since the 1980's**

- | | | |
|------------|------------|--------------------|
| • FAN | STARCIPS-R | STARFIARS-M |
| • ACALS | UCCS | ASIMS |
| • ROC | PBAAS | AIM |
| • SARSS | TIPS | STANFINS |
| • ITP | CSSCS | Army Gateway Prog. |
| • CTASC-II | DAMSS-R | CAISI |
| • CPR | JCALs | ARISS |
| • TADLP | CUITN | SIDPERS, etc... |



Product Evaluation

- **Product Evaluation**
 - **Comprehensive evaluation of candidate products to determine their ability to meet specific operational and technical requirements**
 - Believe it or not, not all vendors or glossy brochures tell the full truth
 - A key to providing professional security engineering services is the ability to know whether or not a candidate solution will actually work in a given environment with specific technical and operational requirements
 - This avoids future program delays that often occur during integration when you find for the first time that the product does not work as the salesman said it would.
 - **The ISEC TIC is DOD's premier Product Evaluation Facility**

CECOM Bottom Line: THE SOLDIER



Product Evaluation (cont)



ISEC has performed product evaluation on the following information assurance items:

- TCP/IP Wrappers
- STU III over ISDN
- Security Audit Reduction/Viewing Tool
- Sun's SunScreen
- SPF-100
- SPI
- SATAN
- DES for Windows
- TEED
- Layer 4 Switching
- Firewalls:
 - SunScreen, PIX, Raptor, Checkpoint (in prog)
- Axent ESM/ITA
- STAT
- CacheFlow Web Proxy
- Cisco Cache Engine
- Trend Micro Content Filter
- Secure DNS
- INKTOMI Traffic Server Web Cache, etc...



Modeling and Simulation



- **Modeling and Simulation**

- The use of models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making managerial or technical decisions.
- **A well developed model and subsequent simulation of real world issues will save development time and cost**
 - ISEC is developing OPNET model for PKI Directory Architectures and DMS Messaging
 - Authored and presented White Paper “Modeling and Simulation Techniques for Comparing PKI Directory Architectures in a Military Environment”



Certification Testing



- **Certification**

- **“Comprehensive evaluation of the technical and non technical security features of an AIS 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.” AR 380-19**

- Certification testing is undertaken to obtain an impartial statement on the ability of a given system to satisfy it’s security requirements.
- ISEC realizes that system developers and owners have limited resources and must make tradeoffs.
 - We report the findings, but rely on the DAA to determine whether or not the security is “good enough”



Certification cont.



- **ISEC History**

- Like Security Engineering, ISEC has been performing Security Certifications for quite some time

- ITP
- SIDPERS 3 (with 5 follow ons)
- ARISS
- SBIS (with 3 follow ons)
- TADLP Block 1 TADLP Block II
- Carlisle Barracks ISM
- ISM CIF Fort Carson, etc...



Certification cont.

- **ISEC FY01 Certification Activities**

- **PEO STAMIS Support:**

- TADLP Blocks II & III MC-4 Block I
- GCSS-A Tier 1 JCALS SWP-3
- TCAIMS-II HSMS
- PERSTEMPO MTS Block II
- SARSS 1/2AD

- **CUITN CANs**

- Fort Alaska Fort Hawaii
- Forts: Polk, Riley, Benning, Dix, Eustiss, McPherson, Sill, Lee
- Rock Island, Redstone Arsenal, Anniston AD



IA Functional System Support



- **IA Functional Systems**

- **While systems of all functional purposes require security engineering and certification support, some systems in themselves perform security functionality**

- **Defense Message System**

- ISEC is the Army's chief DMS implementer
- ISEC has been responsible for the commissioning of 88 DMS sites in CONUS, USARPAC, Korea and SWA

- **Medium Grade Messaging System (MGS)**

- MGS will take the place of DMS for the individual user
- Integrates capabilities of existing email systems with PKI
- ISEC is developing a MGS Implementation Plan for AMC

- **Secure Single Sign (S3) On**

- ISEC is developing a S3 capability for AMC Web Sites



IA Infrastructure Support



- **Infrastructure**

- “An underlying base or foundation; the basic facilities, equipment, and installations needed for the functioning of a system”

- **In the Army’s IT environment this means the network and systems required to provide support to interconnected information systems**
- **ISEC has two major on-going projects to provide security support to Campus Area Network level infrastructures**
 - **Army Materiel Command Security Engineering Assessments**
 - **Common User Installation Transport Network**
- **Additionally ISEC provides the IA technical support to the I3A IA Working Group**



IA Infrastructure Support cont.



- **Army Materiel Command**
 - ISEC provides on site security engineering assessments including the following activities:
 - Technical Vulnerability Assessments
 - Critical Server hardening
 - Critical System Evaluation
 - Business Practice Review
 - Policy Compliance and Practices
 - Network Security Design
 - Map Infrastructure Network
 - Develop Integrated Network Security Design
 - **This is a comprehensive system approach to a CAN**



IA Infrastructure Support cont.



- **Army Materiel Command**

- Evaluations have been conducted at:

- Redstone Arsenal TACOM
- Rock Island Arsenal Aberdeen Proving Ground
- Army Research Lab STRICOM
- HQ, AMC Tobyhanna
- Lone Star AD Pine Bluff
- Pueblo Rocky Mountain Arsenal
- Sierra Army Depot Picatanny
- Red River Watervliet
- Goose Creek Natick, more to come in FY 01

- **Excellent preparation for the Army CAP Requirement**



IA Infrastructure Support cont.



- **Common User Installation Transport Network (CUITN)**
 - ISEC provides security engineering, certification and accreditation support to PM DDN in his CUITN program
 - Same IA efforts as for AMC, with the addition of IA Tool implementation and follow on Certification
 - To date the following sites have been completed or are scheduled:
 - Carlisle Barracks (completed, accredited, and independently evaluated)
 - Fort Carson, CO
 - Fort Alaska (all army installations in Alaska)
 - Fort Hawaii, Forts Polk, Riley, Benning, Dix, Eustiss, McPherson, Sill, Lee, Redstone Arsenal, Anniston Army Depot, Rock Island
 - Satisfies Army CAP requirement



IA Infrastructure Support cont.



- **TRADOC Information Assurance Support**
 - In support of the TRADOC DCSIM ISEC is providing periodic technical vulnerability assessments to all the TRADOC installations
 - Carlisle Barracks
 - Fort Benning
 - Fort Gordon
 - Fort Jackson
 - Fort Leavenworth
 - Fort Leonard Wood
 - Fort Rucker
 - Monterey
 - Fort Bliss
 - Fort Eustis
 - Fort Huachuca
 - Fort Knox
 - Fort Lee
 - Fort Monroe
 - Fort Sill



IA Infrastructure Support cont.



- **I3A IA Support**

- ISEC provides the technical leadership to the Army's I3A IA Working Group.
- Working with the DISC4 leadership and the IA Working Group ISEC has undertaken the following tasks:
 - SIPRNET Security Review- Fort Stewart
 - Security Review of the Army CONUS TNSOC
 - Malicious Mobile Code Detection Pilot Testing
 - Wireless and Portable Electronic Device IA Review
 - Data Confidentiality Requirements Study
 - Mail Gateway Feasibility Study
 - Top Level Architecture Re-Design
 - Connection Approval Process



IA Infrastructure Support cont.



- **Pentagon Engineering Support**

- ISEC, through it's Pentagon Engineering Field Office, is providing full IT support, including IA, to PM IM&T/Renovation for the Pentagon's Renovation Effort
 - C&A Documentation
 - ST&E Testing
 - Physical security in support of the Defense Protective Service
 - SCIF support in coordination with DIA
 - Network Security Architectures and Assessments
 - Vulnerability Assessments, in coordination with NSA, on the Pentagon Backbone



IA Infrastructure Security Success Examples



- **Common User Installation Transport Network**
 - Security Integrated in ICAN design in support of PM DCASS
 - **Carlisle Barracks**
 - First incorporation of full scale ICAN Security Design
 - Successful independent verification of implemented design by CSC, Inc and Land Information Warfare Activity
 - **Fort Carson**
 - Follow on CUITN site incorporating enhanced security
 - e.g., Network Demilitarized Zones
- **Secure DNS**
 - Coordinated effort between ISEC and Army Signal Command to design, test and install new secure DNS for the Army



ISEC: The Army's IT "Go To" Command



- **Office of the Secretary of Defense (Jul 99)**
 - **An improperly implemented security design for the OSD Campus Area Network failed**
 - **DepSecDef set a deadline for repair and the Army called in ISEC**
 - ISEC provided Security Engineering and Architecture Leadership; Firewall and Network experts; and experienced implementers
 - The work was done ahead of deadline with minimal outages at 'turn on'
- **ISEC is prepared to respond immediately to DoDs needs**



Summary



- **Information Assurance is not a discrete event**
- **Information Assurance is achieved only after a thoughtful, holistic systems approach has been applied to securing the system**
- **Information Assurance is maintained only when the total system lifecycle is considered and appropriate policies, safeguards, resources and management interest is maintained**
- **C&A only provides assurance and an administrative approval, by itself it does not secure a system**



Conclusion

- **ISEC represents the single organization in the Army that:**
 - **Provides full spectrum Sustaining Base Information Assurance support**
 - **Integrates IA into the complete system engineering solution**
 - **Provides one stop shopping for all IA technical assistance from Requirements Definition and Satisfaction through Certification and Accreditation**
 - **The ISEC POC is:**
 - Mr. Ted Hendy
 - DSN 821-2855
 - hendyt@hqisec.army.mil