



Information Assurance

17 August 2011

**Chris Denz, AFSPC/A6SA
Keith Gilbreath, AFNIC/EVSN
Vince Williams, AFNIC/EVPC**



Overview

- **General C&A Information**
- **Software Certification Process**
- **Platform IT (PIT) Process and Platform IT Interconnection (PITI)**
- **Change Management**
- **Connection Approval**
- **C&A Training Opportunities**
- **Personnel Slots**
- **Tools**



M&S Problem Statement

- **The M&S community faces several challenges in meeting the current criteria under the current DIACAP and AFCAP for:**
 - **Obtaining software certification**
 - **Completing system certification & accreditation**



Cyberspace Superiority Hierarchy

Service Core Function

Cyberspace Superiority

Missions

Cyberspace Support

Cyberspace Defense

Cyberspace Force Application

Establish and Extend

Passive Defense

Offensive Counter Cyberspace

Persistent Network Operations

Defensive Counter Cyberspace

Secure & Protect

Information Assurance

Global Reach & Access

ISR

Mission Assurance

Influence Operations

Command and Control

Situational Awareness

Capabilities



Air Force CIO Mission



Air Force CIO (SAF/CIO A6)

- **Serve as the senior CIO policy and resources official**
- **Reviews & provide recommendations on:**
 - **Performance of the AF's IT & NSS programs**
 - **AF's budget requests for IT & NSS**
 - **Continuation, modification or termination of IT and/or NSS programs or projects**
 - **Formulation & implementation of enterprise-level defense strategies from the information, IT, network-centric, & non-intelligence space perspective**
- **Develops & maintains SECAF Comm & IT Strategic Plan**
- **Establish & maintain an IM/IT capital planning & investment management process**
- **Serves as AF IM/IT Portfolio Manager**
- **Serves as AF Chief Architect for AF enterprise info environment**
- **Appoints DAAs & SIAO**
- **AF "Senior Communicator" & functional authority for Cyberspace and C&I career fields**



AFSPC – What We Do

• Space

- **Provide Joint warfighting space capabilities**
- **Acquire space systems**
- **Provide assured access to space**
- **Assured capabilities across the spectrum**



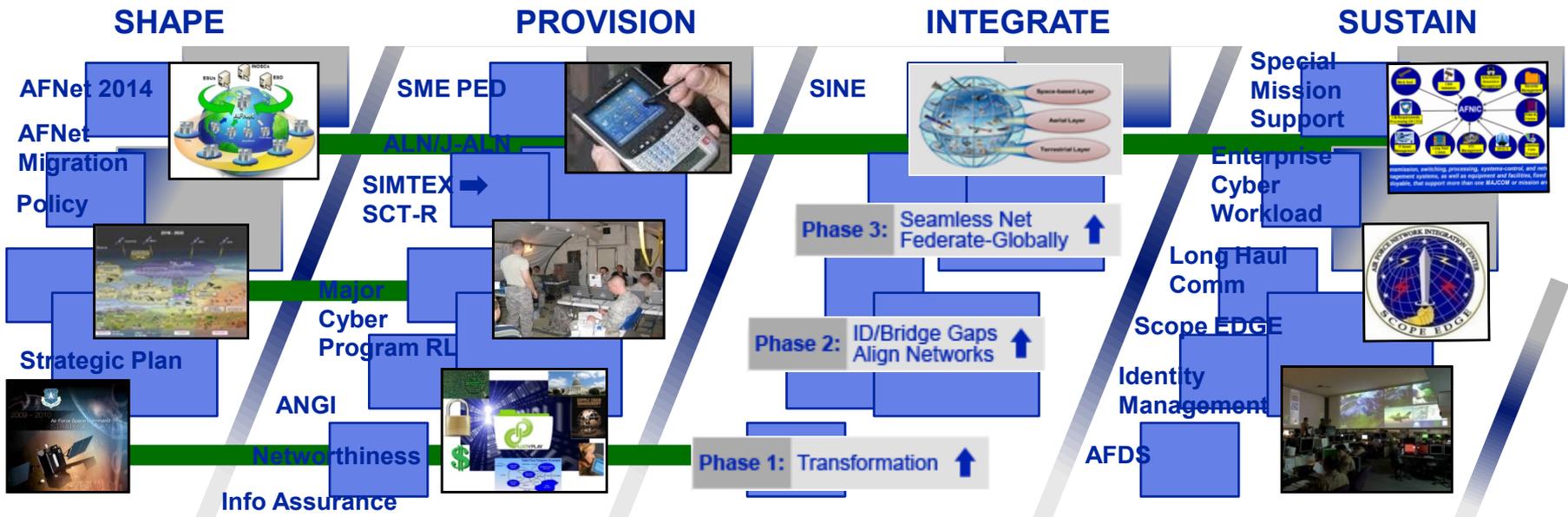
• Cyberspace

- **Present full spectrum capabilities for the Joint warfighter in, through and from cyberspace**
- **Extend, operate and defend the AF portion of the DoD Network**
- **Establish requirements for future cyberspace systems/capabilities**
- **Assured capabilities across the spectrum**





AFNIC Mission





Information Assurance

GENERAL C&A INFORMATION



IA through C&A

- **The process for ensuring IA is Certification and Accreditation**
 - **Certification: a standardized, comprehensive evaluation and validation of an information system to establish the degree to which it complies with assigned IA requirements**
 - Starts with system security design and build
 - Independent testing and design reviews
 - **Accreditation: A formal acceptance of risk associated with operating an information system**
- **The DoD process for C&A is known as DIACAP**

C&A is a “cradle-to-grave” process



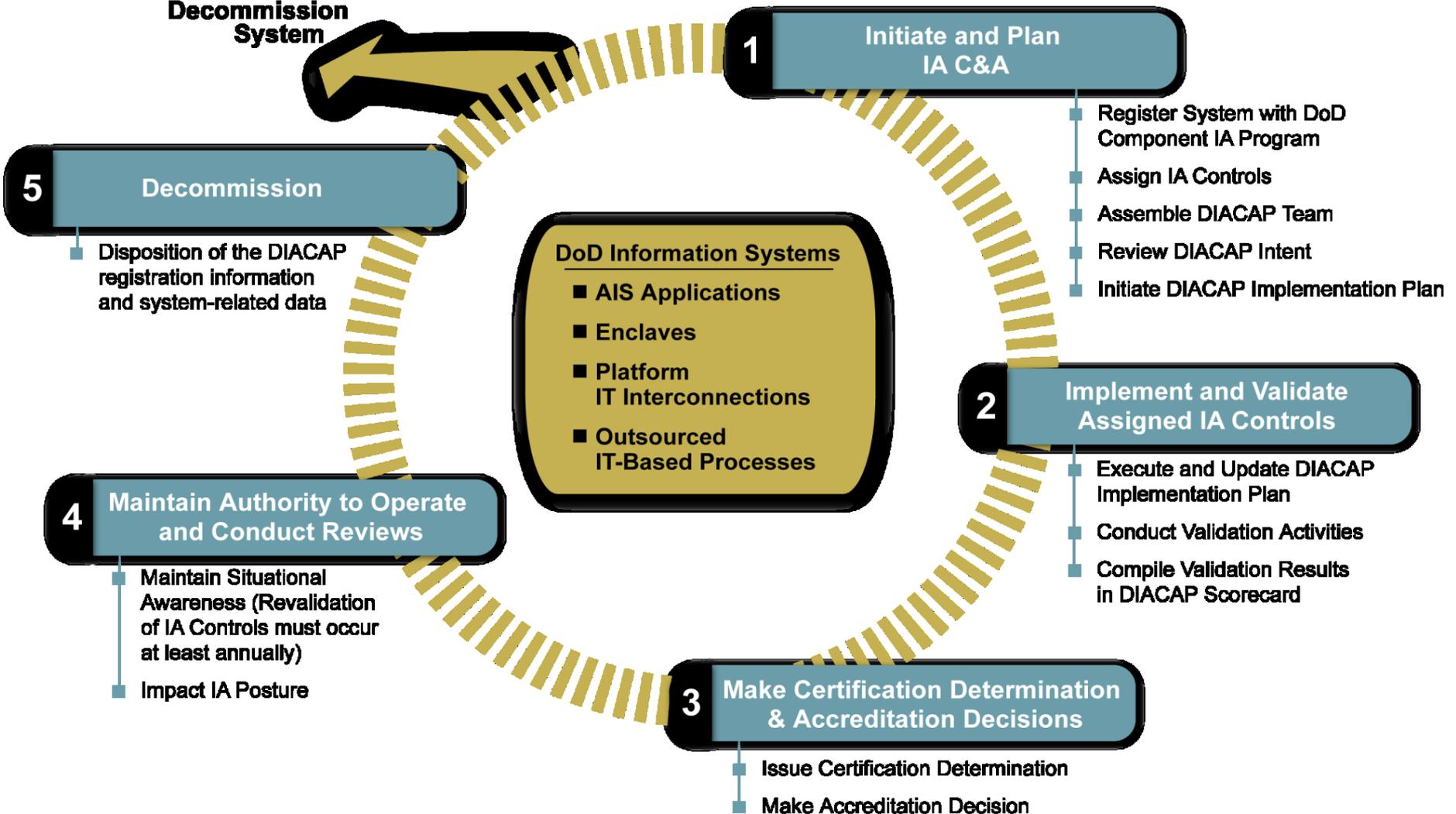
C&A is integral to Mission Assurance

- **C&A goes beyond Net Security—it's about assuring the mission!**
 - ***Confidentiality* = Is my sensitive data secure?**
 - ***Integrity* = Can I rely on the accuracy of my data?**
 - ***Availability* = Will my data/services be available when I need them?**
- **Mission Assurance Category (MAC)**
 - **Fundamental concept upon which current C&A process is designed**
 - **Used in conjunction with the system confidentiality level to determine the IA requirements for a system**
- **IA Controls**
 - **DoD developed these safeguards for developing a system's security design, to assure the mission & secure the network**



The DIACAP Process

Decommission System





Key Roles



Successful C&A requires continued involvement from many



CAs & DAAs That May Be Involved

<u>Area</u>	<u>DAA</u>	<u>CA</u>
Air Force Enterprise	AFSPC/CC (Gen Shelton) • Delegated to AFSPC/A6 (Brig Gen Dickinson)	AFNIC/EV (Mr. Cronin) AFNIC/EV2 (Mrs. Klein)
AF.EDU	AETC/CV (Gen Rice)	AETC/A6 (Col Tucker)
USAFA.EDU	USAFA/CC (Lt Gen Gould)	USAFA/A6 (Ms. Nicks)
Logistics (not all systems)	AF/A4I (Mr. Dunn)	ESC/ENIA
Rapid Cyber Acquisition	AFPEO/C2&CS (Lt Gen Bowlds)	ESC/ENS (Mr. Mayer)
ESC-based Research, Development, Test, and Evaluation	ESC/EN (Dr. Rudolph)	ESC/ENS (Mr. Mayer)
Development Test & Evaluation	AFMC/A3 (Mr. Deis)	AFMC/A3 (Mr. Goddard)
Science & Technology	AFRL/CC (Maj Gen Pawlikowski)	AFRL/CS (Mr. Henry)



Information Assurance
SOFTWARE CERTIFICATION



Background

- **Air Force policy (AFI 33-210) requires all software on the network to be certified**
- **Air Force product sources**
 - **i-TRM**
 - **AIPT/AFNet CCB approved products**
 - **i-TRM products are not certified**
 - **Air Force Evaluated/Approved Product List**
 - **Products issued Certification Memos by the Air Force Certifying Authority**
 - **Products are re-certified for each major release**
- **DoD/Federal product sources**
 - **DISA UC/APL**
 - **USCYBERCOM**
 - **Common Criteria**

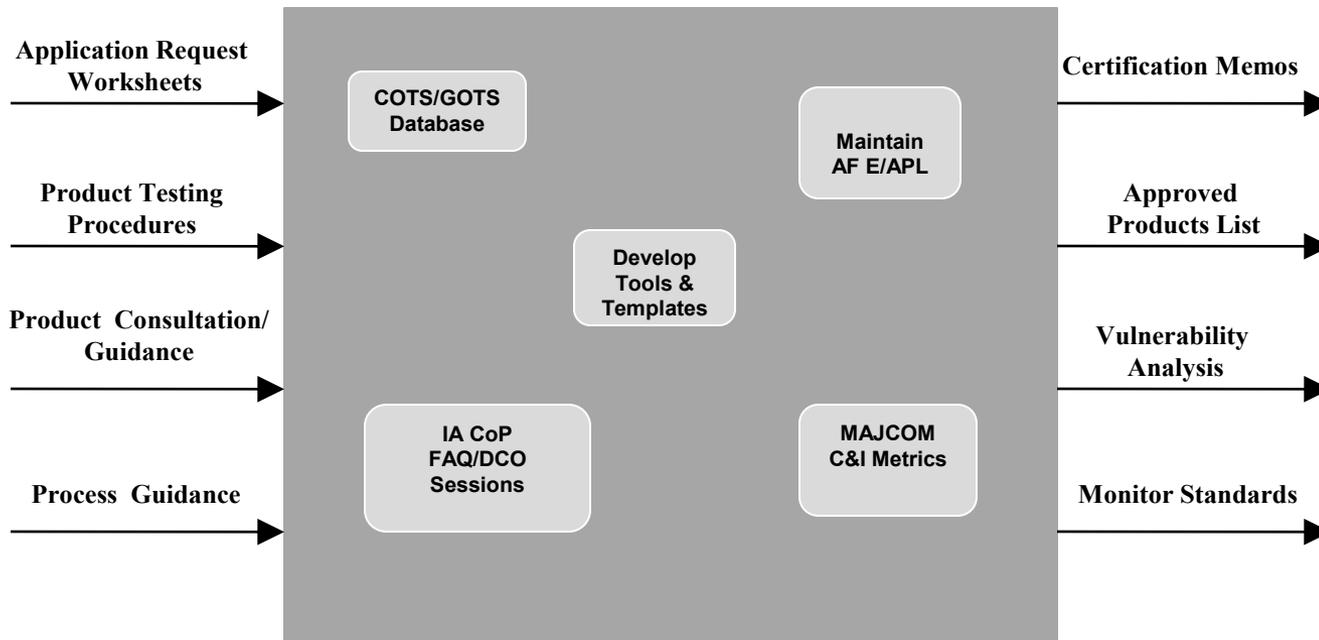


COTS Types

- **Software Applications**
 - PC Desktop
 - Web Server
 - Mobile Devices (e.g., Blackberry, WinMobile)
- **Hardware Devices**
 - Multi-functional Printing, Imaging
 - Broadband Mobile
- **Enterprise Level (Federal/DoD)**
 - IA/IA enabled (e.g., OS, Encryption, Anti-Virus)
 - Unified Capabilities (e.g., voice/video/data)

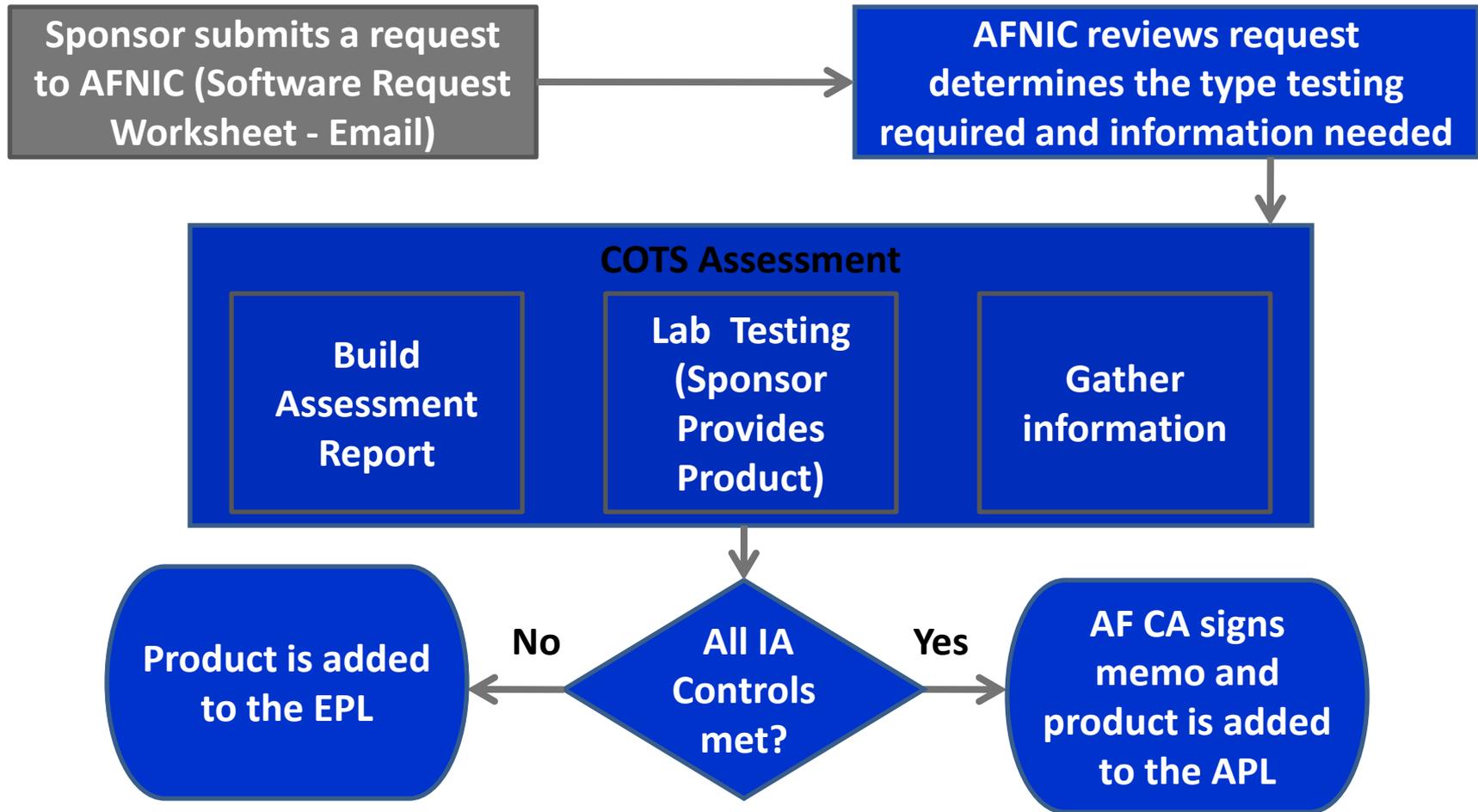


AFNIC's Role





COTS Process





Gather Information

- **Product sponsor submits the software request worksheet**
- **Review Product documentation**
 - **Technical documentation**
 - **User Agreements (auto-updates)**
- **Determine any network resources required to operate**
 - **Are the ports and protocols allowed to be used**
 - **Are there bandwidth issues**
 - **Network Diagrams**
- **Determine software requirements to operate**
 - **May require additional software to be installed**
- **Protection of Data**
 - **Type of Encryption**
 - **Type of Authentication**



Lab Testing

- **Vulnerability Check**
 - Search Vulnerability Databases for known vulnerabilities
- **System Changes**
 - Track all changes made to the system by installing the program
 - What registry and file changes are being made
 - Do these changes impact security of the system?
 - Is this software compatible with the AF's desktop settings
- **Network resources**
 - Perform Captures of network traffic
 - What data is being transmitted?
 - Is the Data being encrypted?
- **Results**
 - What are the risks and can the risk be mitigated?



Example Assessment

- **Rosetta Stone & Speech Recognition Engine**
- **A web based application that allows an user to learn a foreign language**
- **For all features of the application to work the Speech Recognition Engine has to be installed on the user's desktop**
- **Documentation Review**
 - **Application uses HTTP (Port 80) to connect to Rosetta Stone website**
 - **Application uses Adobe Flash 9 in order to interact with the Speech Recognition engine**
 - **Speech Recognition Engine needs administrator rights to install**



Example Assessment

- **Vulnerability Analysis**
 - No known vulnerabilities found
- **System Changes**
 - **Speech recognition engine install 3 exceptions into the Windows Firewall**
 - **RosettaStoneLtdController.exe (TCP 55569)**
 - **RosettaStoneLtdServer.exe (TCP 55568)**
 - **RosettaStoneLtdServices.exe (TCP 55570)**
 - **Application installs a service that automatically starts when the computer boots (RosettaStoneLtdController.exe)**



Example Assessment

- **Network resources**
 - **Web portion of the application uses HTTP port 80 to connect to the Rosetta Stone website**
 - **Speech Component Engine uses 3 ports (55568,55569, 55570) to communicate with the web portion of the application**
 - **Exceptions in the firewall allow the Rosetta Stone services to listen for incoming requests on 55568, 55569**
 - **Determined Rosetta Stone Services only listen to requests originating from the local machine**
- **Results**
 - **The Speech Component installs a persistent service and 3 exceptions into the local Windows firewall**
 - **These ports are open to remote connections but the listening service only responds to requests from the local machine**
 - **This issue is mitigated because the base network's firewall would block access to these ports from a outside source**



Summary

- **Certification is pre-requisite of Accreditation**
 - IT Products – COTS Process (AF E/APL)
 - Systems (AIS, Enclave, PITI, Outsource IT process) – DIACAP (IATO/ATO)
- **Critical areas to avoiding Accreditation delays**
 - Understand your accreditation roles (“the boundary”)
 - Use pre-certified products in system
 - Stay In-Tune with DAA’s guidance
- **Helpful C&A resources**
 - Agent of the Certifying Authority (ACA)
 - Alternate Testing Facilities (ATF)

PLANNING & FLEXIBILITY IS KEY TO C&A PROCESS



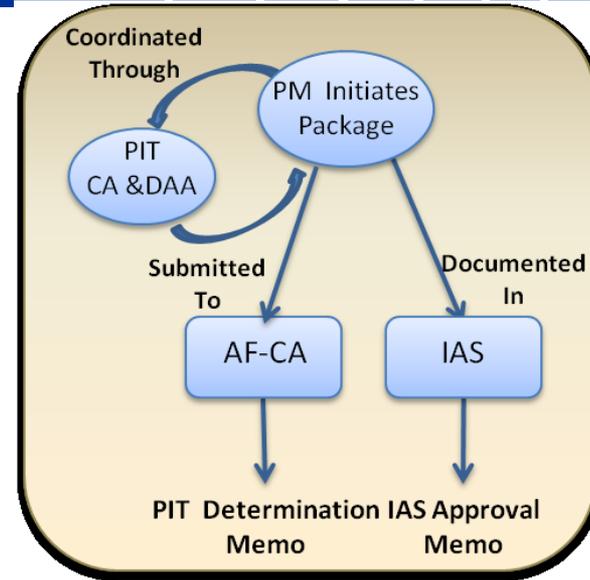
Information Assurance

***PLATFORM IT PROCESS (PIT) &
PLATFORM IT
INTERCONNECTIONS (PITI)***



Platform IT (PIT)

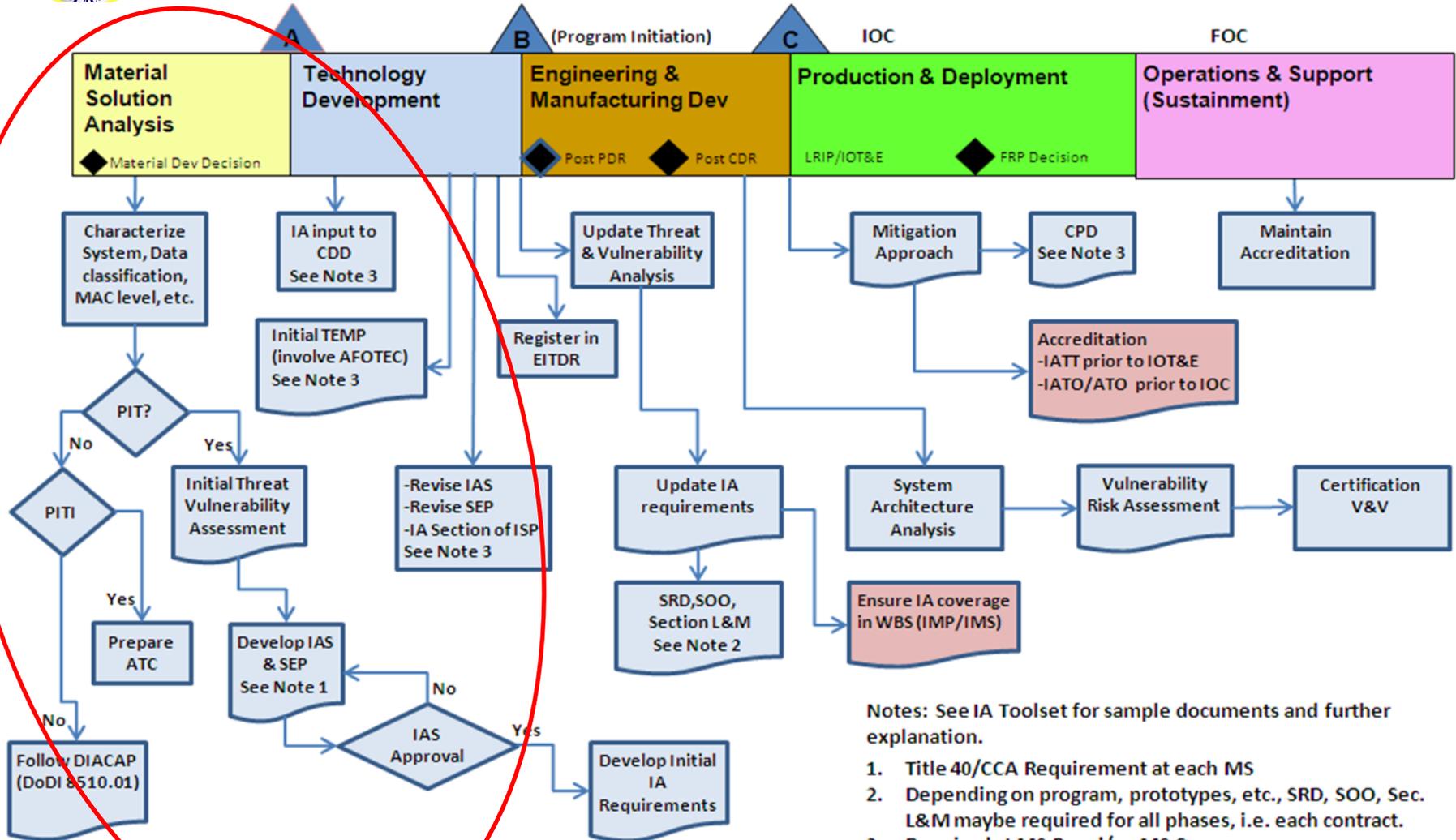
- **PIT Defined:** Computer resources, both hardware & software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as:
 - Weapons
 - Training simulators
 - Diagnostic test & maintenance equipment
 - Calibration equipment
 - Equipment used in the R&D of weapons systems
 - Medical technologies
 - Transport vehicles
 - Buildings
 - Utility distribution systems (e.g. water & electric)



- **Determination Basics**
 - PM submits PIT determination checklist to PIT CA & PIT DAA
 - If concurs
 - With IAS: SAF/CIO A6 will approve
 - Without IAS: AF-CA will approve



PIT and System Engineering



Notes: See IA Toolset for sample documents and further explanation.

1. Title 40/CCA Requirement at each MS
2. Depending on program, prototypes, etc., SRD, SOO, Sec. L&M maybe required for all phases, i.e. each contract.
3. Required at MS B and/or MS C



Risk Management

- **PIT IA risks must be identified and assessed**
 - **PMs must establish IA risk mgt program**
 - **Utilizing a multi-disciplined Integrated Product Team**
 - **Input's to overall integrated risk management plan**
- **PIT DAAs are required to formally declare that each PIT system is approved to operate at an acceptable level of risk**
 - **Risk Acceptance must be clearly documented**
 - **Traditional IA documentation (IATT/IATO/ATO) or**
 - **Traditional systems acquisition documentation (MS decision)**



Establishment of AF PIT CAs & DAAs

- **PIT DAAs and CAs**

- Required to complete training; Not required to hold an Industry Certification (CISSP, etc.)
- Independent from Acquisition Program Offices
- DAA: General Officer/SES (or equivalent)
- DAAs assigned by SAF/CIO A6
- CAs assigned by AF SIAO

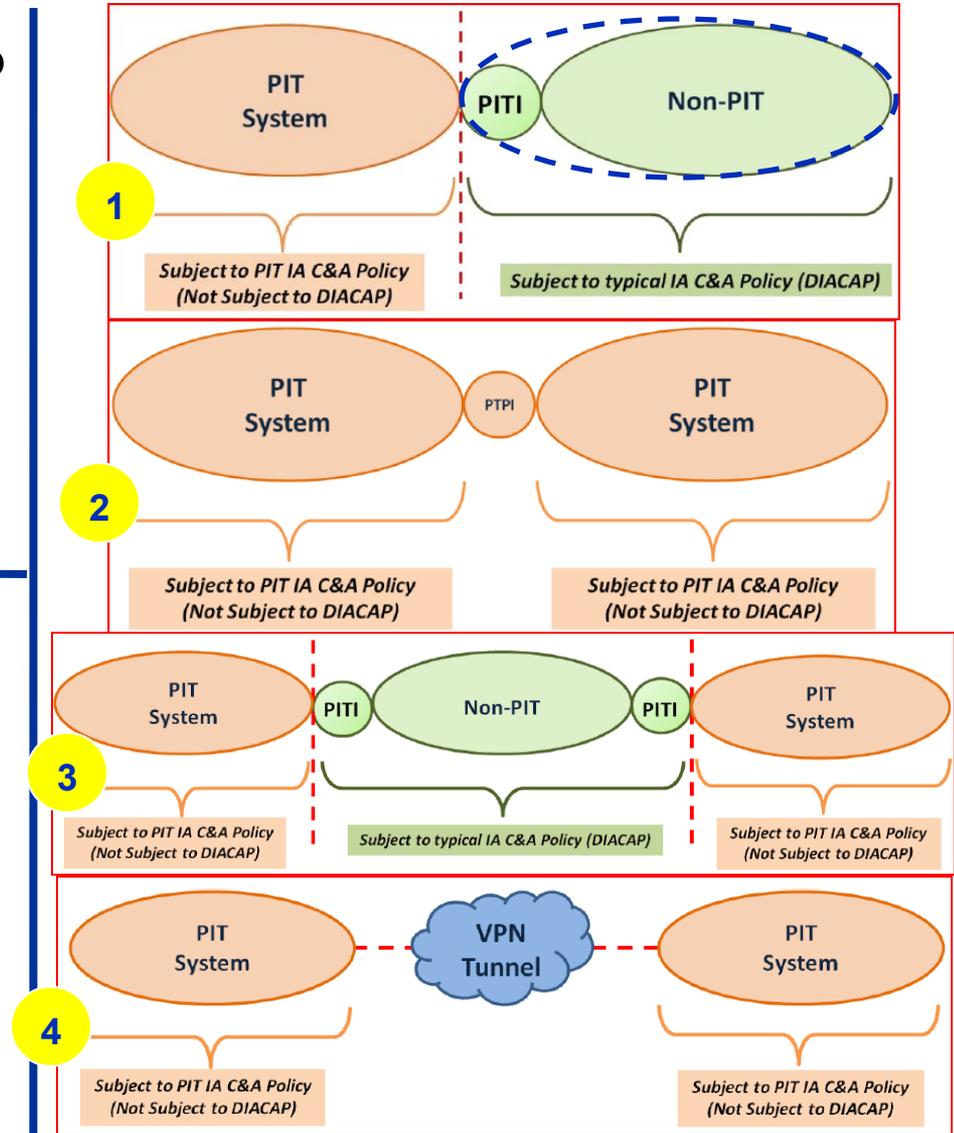
<u>Area</u>	<u>PIT DAA</u>	<u>PIT CA</u>
Aircraft Systems	ASC/CA (Mr. Freisthler)	ASC/EN (Dr. Patel)
Command & Control	ESC/EN (Dr. Rudolph)	ESC/ENS (Mr. Mayer)
Industrial Control Systems	AF/A7C (Mr. Correll)	AFCESA/CEO
Medical	AFMSA/CC (BGen Carroll)	AFMSA/SG6 (Col Zarate)
Weapon Systems	Pending	Pending



Platform IT Interconnection (PITI)

- PITI refers to network access to platform IT

- PITI requires DIACAP accreditation
 - Add it to an existing system's accreditation is the easiest route





Information Assurance

CHANGE MANAGEMENT



Change Management

- **A change is "an event that results in a new status of one or more configuration items approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. (ITIL)**
- **Non-Network Change**
 - **IAMs are responsible for monitoring the impact to security**
 - **Configuration Control Board process**
- **Network Change**
 - **System CCB**
 - **Request change through 24AF Configuration Assessment Board**
- **Newly discovered vulnerabilities**
 - **CAT I corrected <30 days**
 - **CAT II corrected <90 days**



Information Assurance
CONNECTION APPROVAL



Reciprocity

- DoD defines “Reciprocity” as “the mutual agreement among participating enterprises or components to accept each other’s security assessments in order to reuse IS resources and/or accept each other’s assessed security posture in order to share information.”
- Two types: Enterprise and Non-Enterprise
 - Enterprise requires DSAWG & DISN Flag Panel approvals
 - Non-enterprise is a component-to-component agreement

Reciprocity requires mutual agreement between deploying and receiving components



Common misconceptions of Reciprocity

✘ Reciprocity is quick

- DoD reciprocity policy mandates 9-12 month timeline

✘ An accreditation decision = automatic reciprocity

- Reciprocity requires mutual agreement between deploying and receiving components
- Accreditation is environmentally dependent
- An accreditation decision = DAA's acceptance of risk for all implementations of that system

✘ Reciprocity eliminates any further C&A requirements

- Receiving components must review C&A, issue ATC

There is a distinction between C&A Reciprocity & Reuse



Current Connection Process

ATC Request

- System PM submits request for sponsor to SAF/A6OI
- Sponsor uploads required info into workflow

Evaluation

- AF-CA reps conducts risk assessment of system
- AF-CA reps makes recommendation to AF-CA

ATC Issuance

- AF-CA makes recommendation to AF-DAA (or designee)
- ATC is signed



Areas of Opportunity

- **Net-worthiness/connection approval areas:**
 - **Architecture**
 - **Connectivity / Bandwidth**
 - **Infrastructure Services**
 - **Operations & Maintenance**
- **Assessing each area**
 - **DoD Requirement**
 - **What the Air Force is doing already**
 - **Way Ahead**



Information Assurance

***C&A TRAINING
OPPORTUNITIES***



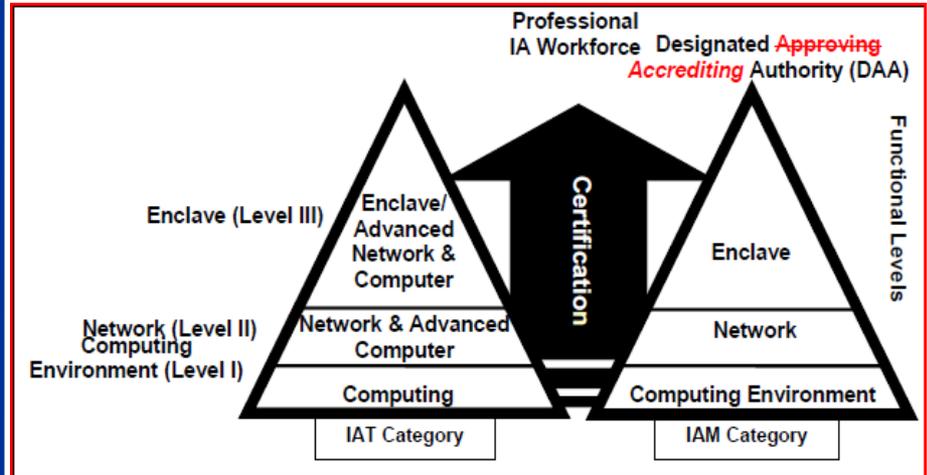
IA Training Requirements

IA functions focus on the development, operation, mgnt, & enforcement of security capabilities for systems & networks.

Personnel performing IA functions establish IA policies & implement security measures & procedures for the DoD & affiliated ISs & networks.

IA Workforce

- **IA Technical** (not comprehensive)
 - Privileged Access
 - Correct flaws in systems
 - Implement technical controls
 - Test IA safeguards
 - Implement IA related patches



- **IA Management** (not comprehensive)
 - Supervise or manage protective or corrective measures
 - Ensure that IS security config guidelines are followed
 - Monitor system performance & review for compliance with IA security and privacy requirements

Total IA Workforce: IAT – IAM – CND-SP – IASAE



IA Training Opportunities

- **“Free” Training**

Personnel in 8570 positions are eligible for access to Software Engineering Institute's Virtual Training Environment (VTE) training material at no cost—DISA funded program.

Eligibility requires that you provide your .mil email address, or the contact information of your supervisor upon requesting access.

<https://www.vte.cert.org/vteweb/>

Air Force
ITE-Learning
HIGH PERFORMANCE TRAINING

SEARCH-and-LEARN®
Search by keywords, title, or ID
Search for: Category: Language:

Shortcuts

- My Plan
- My Favorites
- My Report & Certificates
- My Enrollments
- Student Transcripts
- AF Program Management Office
- User Guide
- Books24x7
- Download Instructions
- Live Help
- Technical Support
- Credentialing
- KnowledgeCenter
- SDC Sponsored MS Training
- DIACAP, PII, IASE Training
- Instructor Led Training

Information

- [My Assignment >>> DoD 8570 IA Certification Support](#)
- [DoD8570 A+ 2009 Technical Level 1](#)
- [DoD8570 Network+2009 Technical Level I](#)
- [DoD8570 Security+2008 Technical Level II](#)
- [DoD 8570 CISSP: Technical Level III](#)
- [DoD8570 Security+2008 Management Level I](#)
- [DoD8570 CISSP Management Level II](#)
- [DoD8570 CISSP Management Level III](#)
- [DoD8570 CEH](#)
- [DoD8570 CISM](#)
- [DoD 8570 Commercial Certification Voucher Request](#)

- **Coded Position**

- AF pays for course
 - Unit pays any TDY
- AF pays for the certification test (1st time)
- AF pays for maintenance fees (developing a process)

- **Non-Coded Position**

May be approved for training and/or certification if 8570 office at AFNIC receives either a digitally signed email or letter from their Commander

<https://private.afca.af.mil/CertifiedWorkForce/index.cfm>



Information Assurance
PERSONNEL SLOTS



Keys to a successful C&A program

A successful C&A effort requires:

- **Trained and experienced C&A/security professionals—not an additional duty**
- **Active involvement of mission owner and program office**
- **Adequate funding—IA is a required budget line item**
- **Starting early—not an end of runway check**
- **A continuous effort—not a once every 3 year event**

Sharing Resources Across the Community May Help



Information Assurance *TOOLS*



Enterprise IT Data Repository

- What is it used for
 - Portfolio Management
 - Linked to DITPR
 - CIO compliance

A screenshot of the EITDR Portal in Internet Explorer. The browser address bar shows "https://eitdr.day.disa.mil/". The page header includes "EITDR" and "AMERICA'S AIR FORCE". The main content area is divided into sections: "Common Tasks" (Add New Record, Browse For Record, Archive/Decommission Record), "Portfolio Management" (PFM Hub, Change Requests), "Quick Links" (EITDR CBAs, EITDR Job Aids, EITDR User Guides, CoP Links, CIO Process Guides, EITDR Training Schedule, eMASS URL, EITDR Training Offerings), "Administration" (Edit User Information, EITDR Administration), and "EITDR Helpdesk" (For Questions: DSN 787-8422, Comm: 937-257-8422). A search bar is visible at the top right. A news section on the right side contains several updates, including a major one dated 30 Jul 2011 regarding EITDR Version 2.13 and a red warning dated 13 Apr 2011 about the discontinuation of C&A Workflow.

News

30 Jul 2011 : EITDR Version 2.13
This server was upgraded to EITDR Version 2.13 on July 29, 2011. Changes include:
• Help Text for All Questions default to "hidden"
• Update to E14 Options Link (blue)
• Include segment architecture & MAJCOM P137 in SNAP-IT Funding Pct Export report
• Lock CY/PY columns in E14
• Restore BN search feature
• FY13BES IAA GIG Category/Data re-alignment
• FY13BES Core Data/Registration Changes
• FY13BES E14 (Resource Data)

13 Jun 2011 : C&A Workflow
Per direction of SAF/IA6 and the EITDR PMO, as of 13 June 2011, C&A Workflow in EITDR is disabled. Data is available as read-only.

13 Apr 2011 : ****C&A Workflow Update****
****The EITDR C&A Workflow will be discontinued based on the email sent from SAF/CIO A6 on 01 April 2011. Please see Policy Guidance (Transition Plan) dated 30 March 2011 advising the implementation of eMASS. Versions that are currently going through C&A will abide by the eMASS transition plan and will be available in EITDR until 01 June 2011. New versions will not be created in EITDR effective close of business, 15 April 11, per the policy guidance. All legacy C&A**

- C&A Data
 - Not used as a C&A workflow
 - Data may still be accessible



Enterprise Mission Assurance Support Service(eMASS)

- **What it is**

DoD's tool used to execute DIACAP in an automated fashion within a workflow construct.

Producing DIACAP artifacts & supports inheritance & reciprocity

- **Why we use it**

- SAF/CIO A6 memo (1 Apr 11)
- Using C&A workflow tool provided by DISA

- **What's coming up**

- Preparing for SIPR IOC date TBD
- Continuing to assist field with questions
- Customer Service Team (DSN 779-6294) answering AFNIC process-specific questions
- AFNIC hosting eMASS forum on the IA COP

- **Contacts for tool issues**

- MAJCOM account managers
- eMASS Help Desk
 - DSN 339-5600

<https://cs.eis.af.mil/a6/emass/Pages/eMASSHome.aspx>

