



DITSCAP to DIACAP MIGRATION

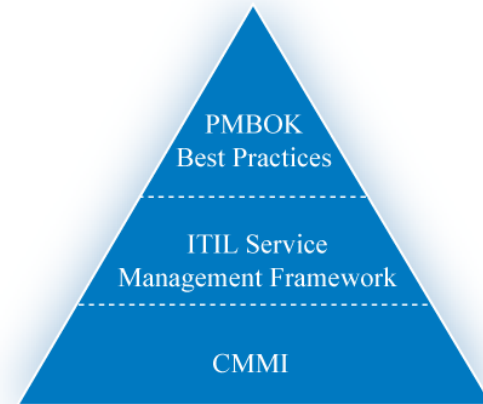
A large, semi-transparent blue graphic on the right side of the slide depicts a person's head in profile, looking down at a notepad. A pen is shown drawing a glowing lightbulb on the notepad. The lightbulb has several short lines radiating from it, suggesting it is lit. The text "Ingenuity at Work" is written in black across the lightbulb.

Ingenuity at Work

Presented by: Thomas E. Gist, Ph.D., CISSP
Presented to: INFOTECH 2007

ATS At a Glance

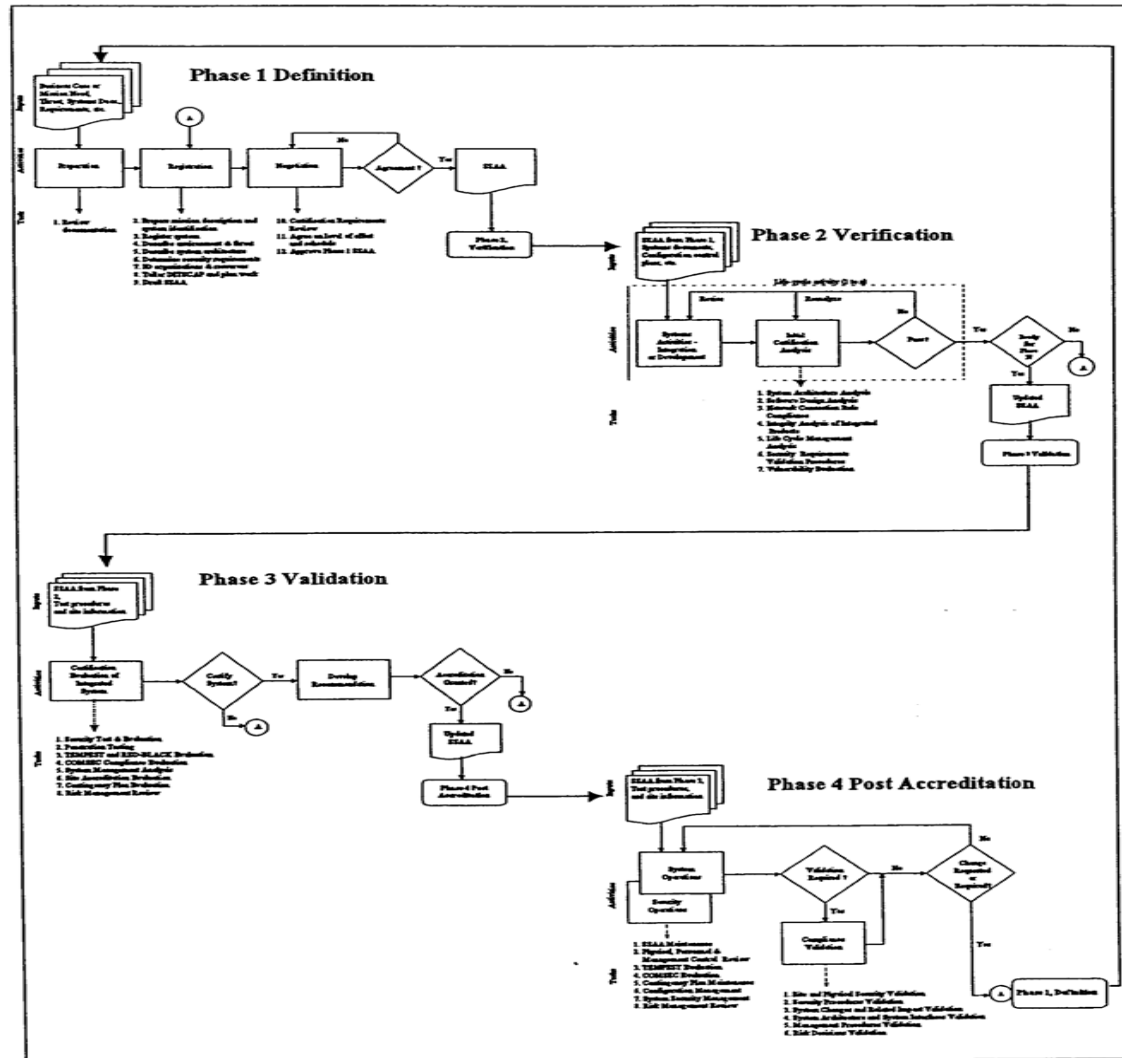
- Information technology solutions provider
- Focused on government solutions
- Founded: 1978
- Revenues: \$100 million
- Staff: 700+
- Office locations nationwide
- CISSP and PMP Certified staff
- The first Government Customer Service Award in the category of "Customer Focus Excellence"
- ITIL® Certified Staff
- ISO 9000, Pursuing ISO 27001
- www.atsva.com



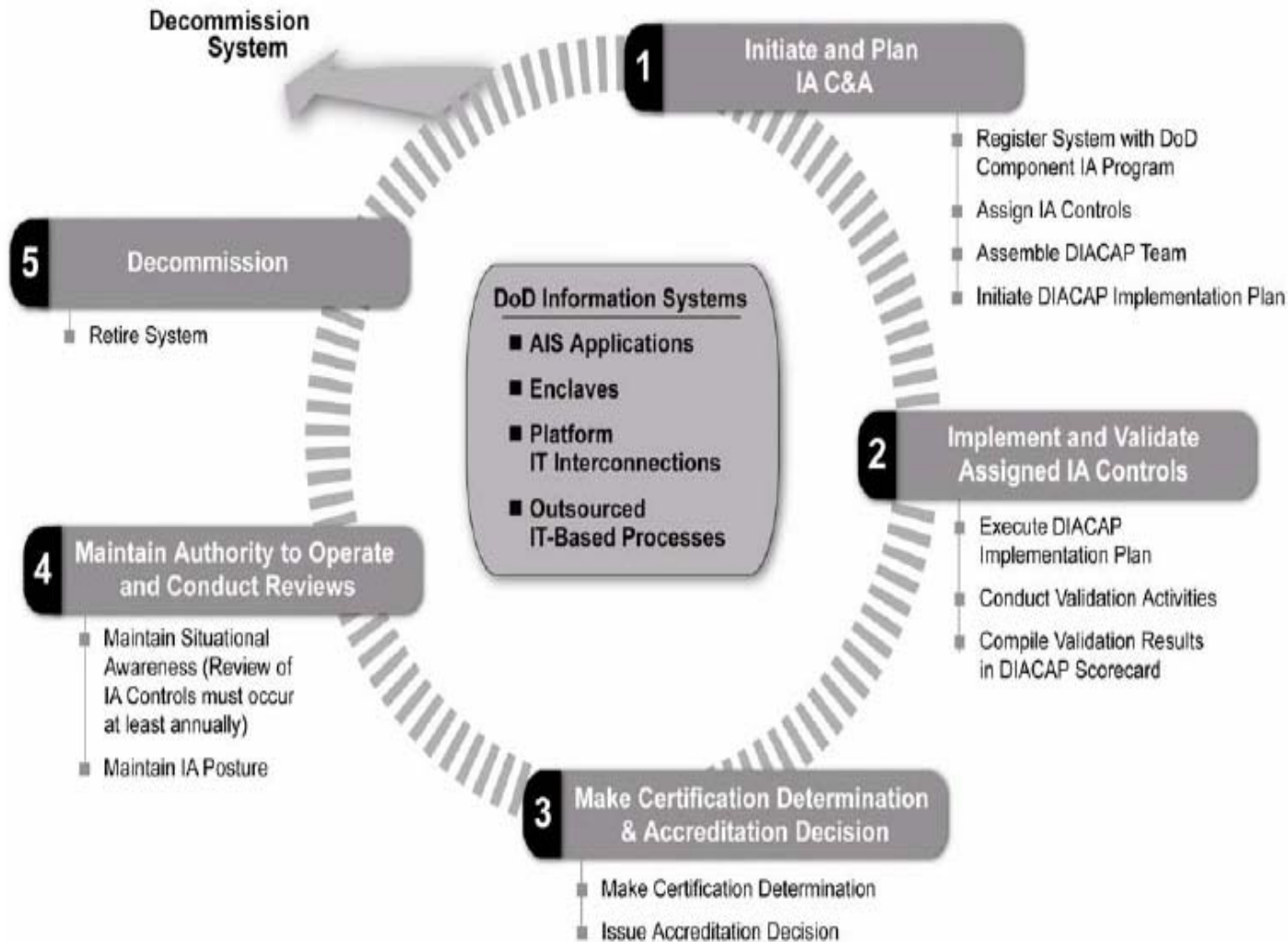
What We Want To Cover Today

- DITSCAP/DIACAP
- DIACAP in Theory
- DIACAP In Practice
- Lessons Learned

DITSCAP/DIACAP



DITSCAP/DIACAP



DITSCAP - Characteristics

- Distributed Process
- Documentation-Based
- Isolationist
- "Plagiaristic"

Sources: DoDI 5200.40
 DoD 8510.1-M

DITSCAP - Distributed

Each Program Has Its Own . . .

- Certifying/Accrediting Officials
 - Problems When Hosted Somewhere Else
- Requirements Set
 - Time-Consuming To Produce
 - Host/Tenant Issues Again
- Testing
 - Very Comprehensive
 - Host/Tenant Issues Yet Again

DITSCAP – Documentation-Based

- SSAA Of Massive Size
 - Six Main Sections
 - 20+ Appendices
 - Includes All The Development Artifacts
 - Often 300 Pages Of SSAA-Specific Text
 - Requirements Traceability Matrix Alone Could Bust 100 Pages
 - “Living Document”
 - Hardcopy Format A Mess To Maintain

DITSCAP – Isolationist

- Couldn't Borrow From Development Artifacts
 - Had To Paste In Architecture Diagrams
 - Had To Include Physical Environment Layout
 - Had To Attach Existing Documents Instead Of Referring
- No Standardized Guidance
 - Requirements: Start Over Each Time
 - Threat Analysis: Start Over Each Time
- No Standards From DAA To DAA

DITSCAP – “Plagiaristic”

- Too Much To Write From Scratch Each Time
- Authors Might Not Have All The Needed Skills
- Steal What You Could
 - Requirements
 - Threat Analysis
 -
- Results:
 - Overkill
 - Square Pegs And Round Holes

DIACAP - Characteristics

- Centralized
- Uses Inheritance
- Emphasis On Automated Support

Sources: DoD Interim Guidance
(Replacement For DoDI 5200.40)

DIACAP Knowledge Service
(Web-Based Replacement For DoD
8510.1-M)

DIACAP - Centralized

- Control
 - Single DAA Per Service (With Some Delegation)
 - All Services Use Common Processes (In Theory)
 - DoD Provides Single Web Reference For All Questions
- Process
 - All Systems Use A Single Threat Analysis (And, In Fact, It's Not Even Included In The Package)
 - All Systems Use A Common Baseline Requirements Set ("DIACAP Controls")
 - Details Are Very Flexible

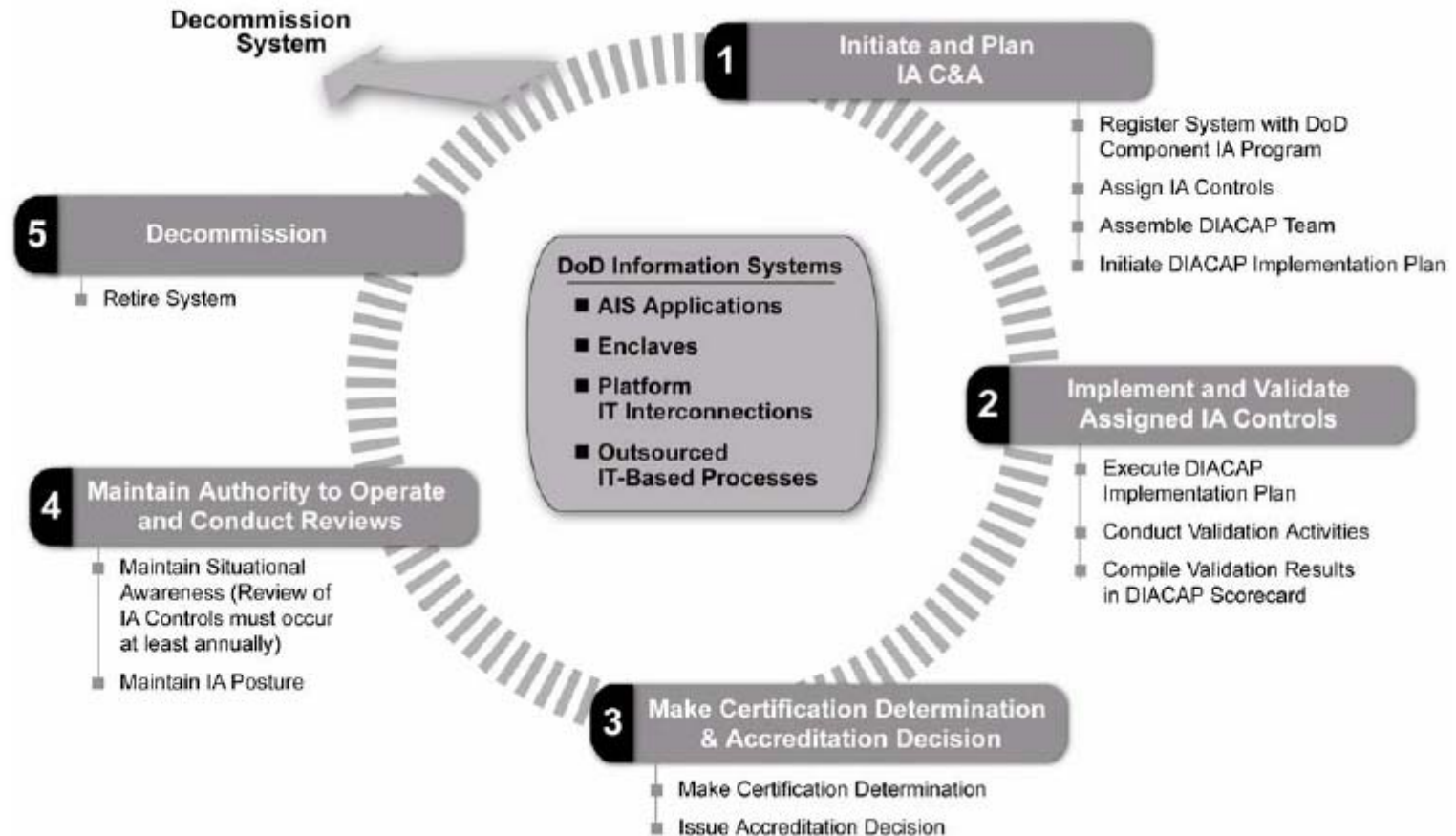
DIACAP – Inheritance

- You Inherit Controls From Somewhere Else
 - “.. Control’s Validation Results And Compliance Status,...”
 - Typically, From The Enclave The Servers Sit In
 - Or From The Network You Travel Over
- You Don’t Test What You Inherit
- You Don’t Document Inherited Controls
 - Provide Results And Compliance, But No Other Details
- Your DAA Accepts The Decision Of Others
 - Some Issues On Non-Compliant Inherited Controls

DIACAP – Automated Support

- Ideally, No Paper Documents At All
- eMASS Is The Standard DoD Automated Tool
 - Automates Steps
 - Stores Information
 - Serves As The Authoritative Source
- Agencies Can Use Their Own Tool
 - AF Uses EITDR
- Various Third-Party Tools Available

DIACAP – In Theory



DIACAP – In Theory

- Determine The Players
- Determine The Controls
 - MAC Level
 - Sensitivity
 - Inheritance
- Validate Controls
 - Ignore Inherited
 - Very Little “Testing”
 - Mostly Done By End Of Build
- “It’s Never Over ‘Til The Paperwork’s Done”

DIACAP Package

- System Identification Profile*
 - Short And Standardized
 - Describes The System
- Implementation Plan
 - Short And Standardized
 - What's Inherited, What's To Be Implemented, And When

** Executive Package That Goes To DAA*

DIACAP Package Take Two

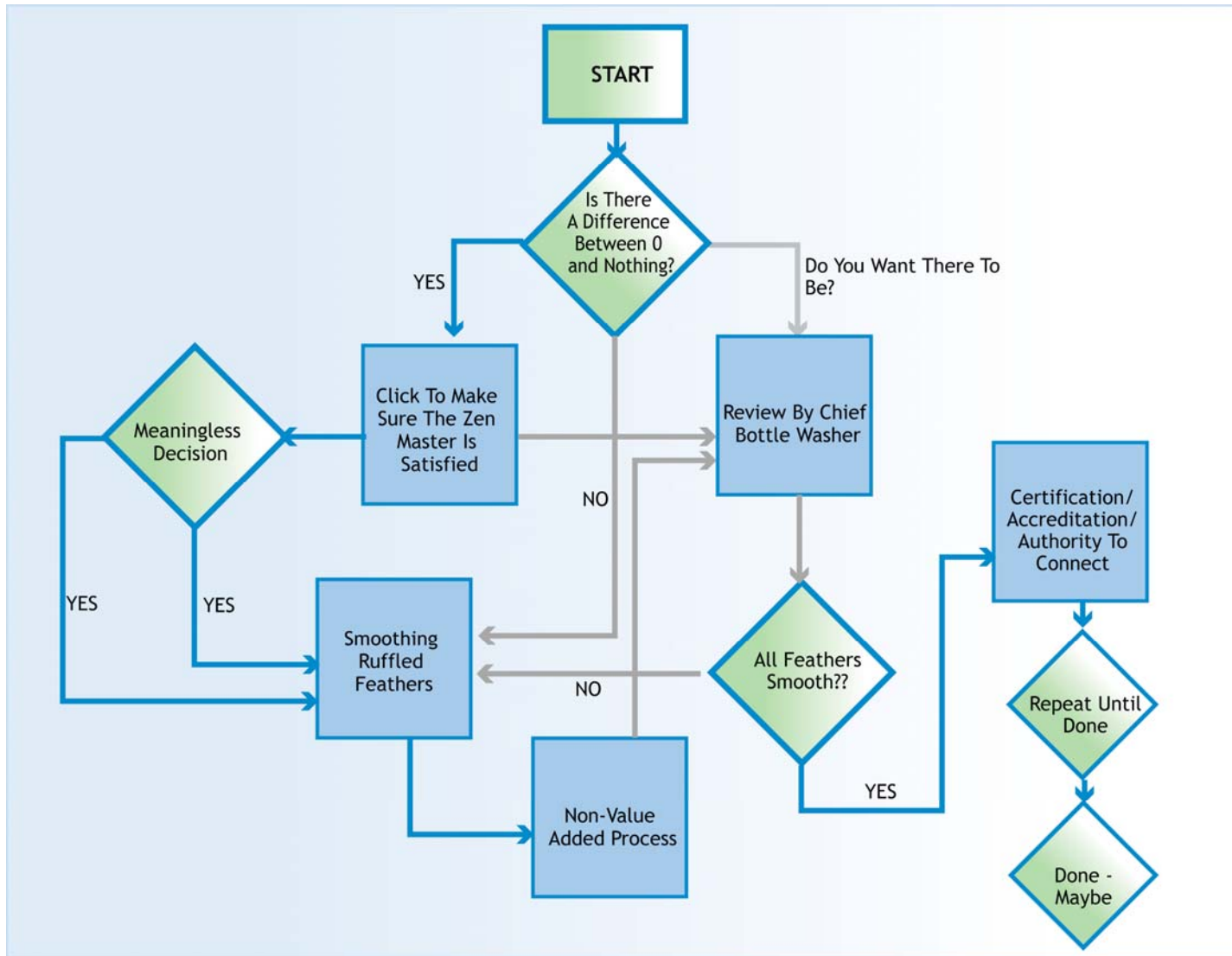
- Scorecard*
 - Short and Standardized
 - Final Results Of Each Control
 - C&A Decision
- Plan Of Action And Milestones*
 - Only Controls Requiring Corrective Action
- Certification Documentation
 - Everything Else

* *Executive Package That Goes To DAA*

DIACAP – Completing The Process

- Certifying Authority Validates The Controls As Being Properly Implemented Or Inherited
- CA Presents Results, Including Residual Risks, To DAA
 - Doesn't Present Implementation Plan, Certification Documentation
- Delegated Accreditation Authority Makes Accreditation Decision
 - Balances Protection Versus Mission/Business Need
 - ATO/IATO/IATT/DATO

DIACAP – In Practice



DIACAP – Process Uncertain

- In AF, AFCA Approves Connection To Network, Independent Of C&A
 - Not Yet Clear Where And When This Occurs
- AF Guidance On Who's On First Does Not Yet Match Practice
 - AFCA Should Be CA
 - **Weren't Able To Get The Pieces In Place**
 - AFNETOPS/CC Should Be DAA
 - **Weren't Able To Get The Pieces In Place**
- Different Chains Of Command
 - CA, DAA, ATC Grantor In Different Commands
 - Final AF Result: CA Grants ATC, But Doesn't Work For DAA

DIACAP – Dissatisfaction

- What Goes Where
- DAAs Or Their Reps Unhappy With Accepting Risks On Non-Compliant Controls
 - Scorecard Doesn't Include Information On Mitigation Or Residual Risk
 - Certification Documentation Doesn't Go Beyond CA
 - Even Worse If Non-Compliant Control Is Inherited
 - POA&M On Every Non-compliant Control

DIACAP – Guidance VS Need

- To Quote The Interim Guidance:
 - Inheritance: When An “IA Control Along With The Control’s Validation Results And Compliance Status, Is Shared...”
 - **Doesn’t Include Mitigation Or Residual Risk Information**
 - POA&M “Required For Any Accreditation Decision That Requires Corrective Actions”
 - **If The DAA Accepts The Risk, No Corrective Action Or POA&M Is Necessary**
 - These Don’t Support The DAA’s Needs

DIACAP – Mechanical Issues

- Knowledge Service Still Debugging
 - Obvious Mistakes In Validation Procedures
 - **No Other Authority To Fall Back On**
 - Errors Between KS And 8500.2
 - No Good Mechanism Yet To Correct Substantive Errors
 - **Must Go To Technical Advisory Group**

DIACAP – Mechanical Issues

- Automated Tools Not Standardized
 - DoD Says eMass
 - Doesn't Require It
 - Doesn't Provide It
 - AF Says EITDR
 - Needed To Prevent Duplicate Info
 - Very Limited Access
 - Not Sure It's Caught Up Yet

Lessons Learned

- There's Lots Of Disagreement On What DIACAP Really Is
 - Well-intentioned, Sincere, But Real Differences
- Guidance Is Ahead Of Implementation
 - And Vice-Versa, To Some Extent

What I'd Do If I Were You

- Define The Team As Soon As Possible
 - DAA/DAAR
 - CA/CAR
- Define The Process As Soon As Possible
 - Make Sure Everyone Agrees On What Everything In DIACAP Means
 - Agree On Where ATC Occurs In The Process
 - Agree On What The Various Players Need In The Way Of Documentation

References

- DoDI 5200.40
<http://www.dtic.mil/whs/directives/corres/pdf/520040p.pdf>
- DoD 8510.1-M
<http://www.dtic.mil/whs/directives/corres/pdf/851001m.pdf>
- DoD Interim Guidance
<http://iase.disa.mil/ditscap/interim-ca-guidance.pdf>
- Knowledge Service: <https://diacap.iaportal.navy.mil>
(Required CAC Or External Certification Authority Certificate)

Last Things Last

Q & A

