

www.TrustedCS.com

Certification and Accreditation (C&A) Basics

Steve Welke
swelke@TrustedCS.com

TCS Company Background



Founded 1994

13 Years of Sustained Profitable Growth

- Locations in VA, IL, and TX

Large SecureOffice® Installed Base

- Government Agencies
- Commercial Enterprises

Recognized Leader in Cross Domain Solutions

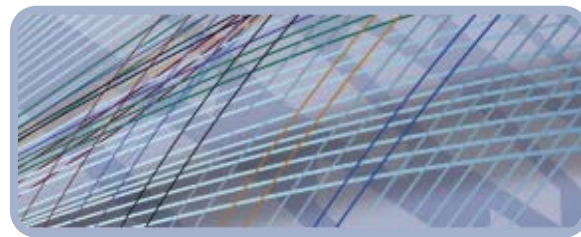
- Original developer of the DoDIIS Trusted Workstation (DTW)
- Cross Domain/High Assurance data access & transfer solutions
- Professional Services Organization
- In-house certification and accreditation department

Proven Security Certification & Accreditation (C&A) Capabilities

- Over a decade of fielding operational systems worldwide
- Superior SABI and TSABI experience



Topics



- C&A Principles
- Overview of C&A Approaches
 - DITSCAP to DIACAP
 - DCID 6/3
 - NIST (based on FISMA)

} DNI / CNSS
- Overview of Cross Domain Solution (CDS) C&A Processes
 - SABI/CDS
 - TSABI

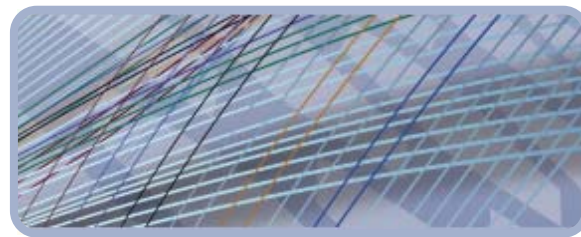
} UCDMO

C&A Principles



- Why C&A?
- What is C&A?
- Why a Common Approach?
- Components of C&A
 - Roles
 - Activities
 - Documents
- Getting Started

Why C&A?



- Systems are comprised of resources, and threats to and vulnerabilities in those resources affect:
 - The ability to perform missions
 - Lives
- Threats and vulnerabilities create risks, which motivate the security requirements/controls and design of the system
- The residual risks that remain once the system is complete must be assessed before approving the system for operation

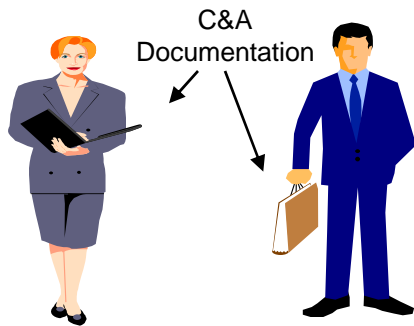
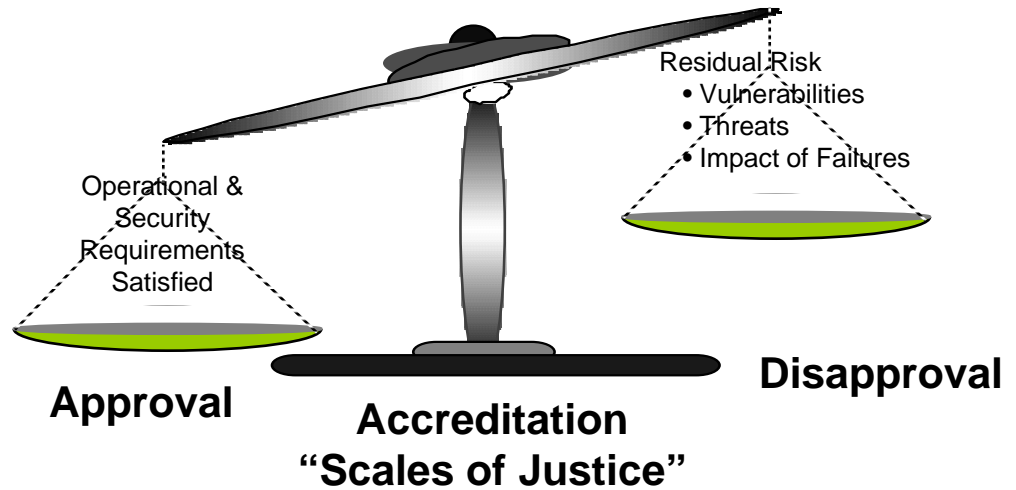
What is C&A?



- **Evaluation:** a technical analysis of a product's protection features, independent of any mission or operational environment, against a stated criteria.
- **Certification:** an assessment of the technical and non-technical features of a system to establish the extent to which it meets a set of security requirements/controls in a particular operational environment.
- **Accreditation:** the official administrative approval that is granted to a system to process sensitive information in its operational environment.

C&A is an informed approach to managing risk

The Trial: Operational Utility vs. Risk



Certification Evidence Generators
"The Defense Lawyers"



Why a Common Approach?



- Everyone was doing C&A their own way, causing confusion from project to project
- C&A Approaches
 - DITSCAP to DIACAP
 - DCID 6/3
 - NIST (based on FISMA)

} DNI / CNSS
- Cross Domain Solution (CDS) C&A Processes
 - SABI/CDS
 - TSABI

} UCDMO

A common approach to conducting and documenting C&A facilitates understanding and reuse

Components of C&A

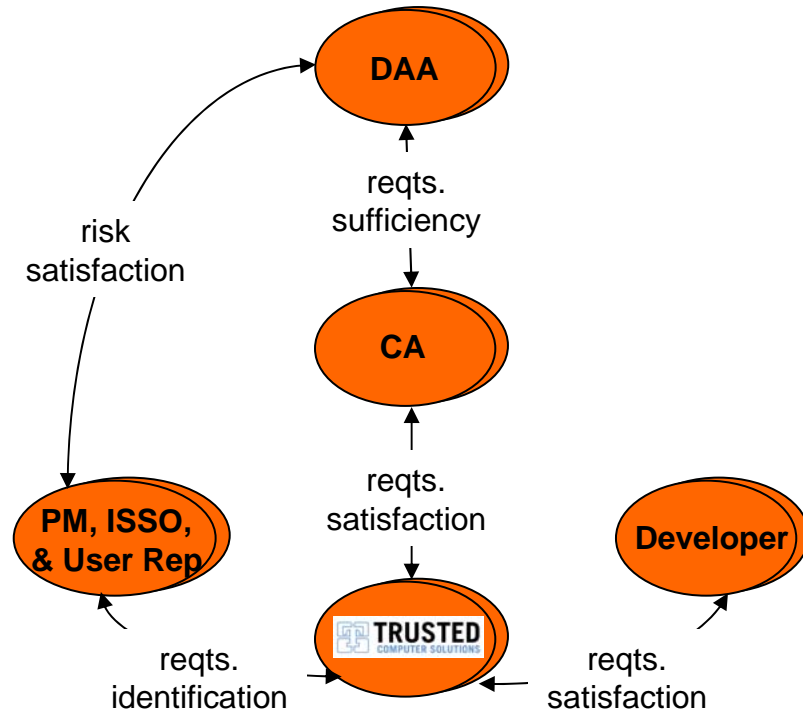


- **Roles**
 - Essentially the same between different approaches
- **Activities** (grouped in phases)
 - Essentially the same between different approaches
- **Documents**
 - Same content in each approach, but captured in different ways

C&A Roles



- Key Roles
 - DAA
 - CA
 - PM
 - User Rep
- Additional Roles
 - ISSO/ISSM
 - Developer
 - C&A Facilitator (TCS!!)



C&A Activities



Phase

Goal(s)

Phase 1 (Pre-Certification): understand the environment, mission, and architecture to determine the security requirements and effort necessary for accreditation

- Develop majority of evidence
- Define requirements

Phase 2 (Certification): verify the evolving or modified system's compliance with the information agreed upon during Phase 1

- Develop tests

Phase 3 (Accreditation): validate the fully-integrated system's compliance with the information in the SSAA

- Execute tests
- Analyze residual risk

Phase 4 (Post-Accreditation): those activities necessary for the continuing operation of the accredited system

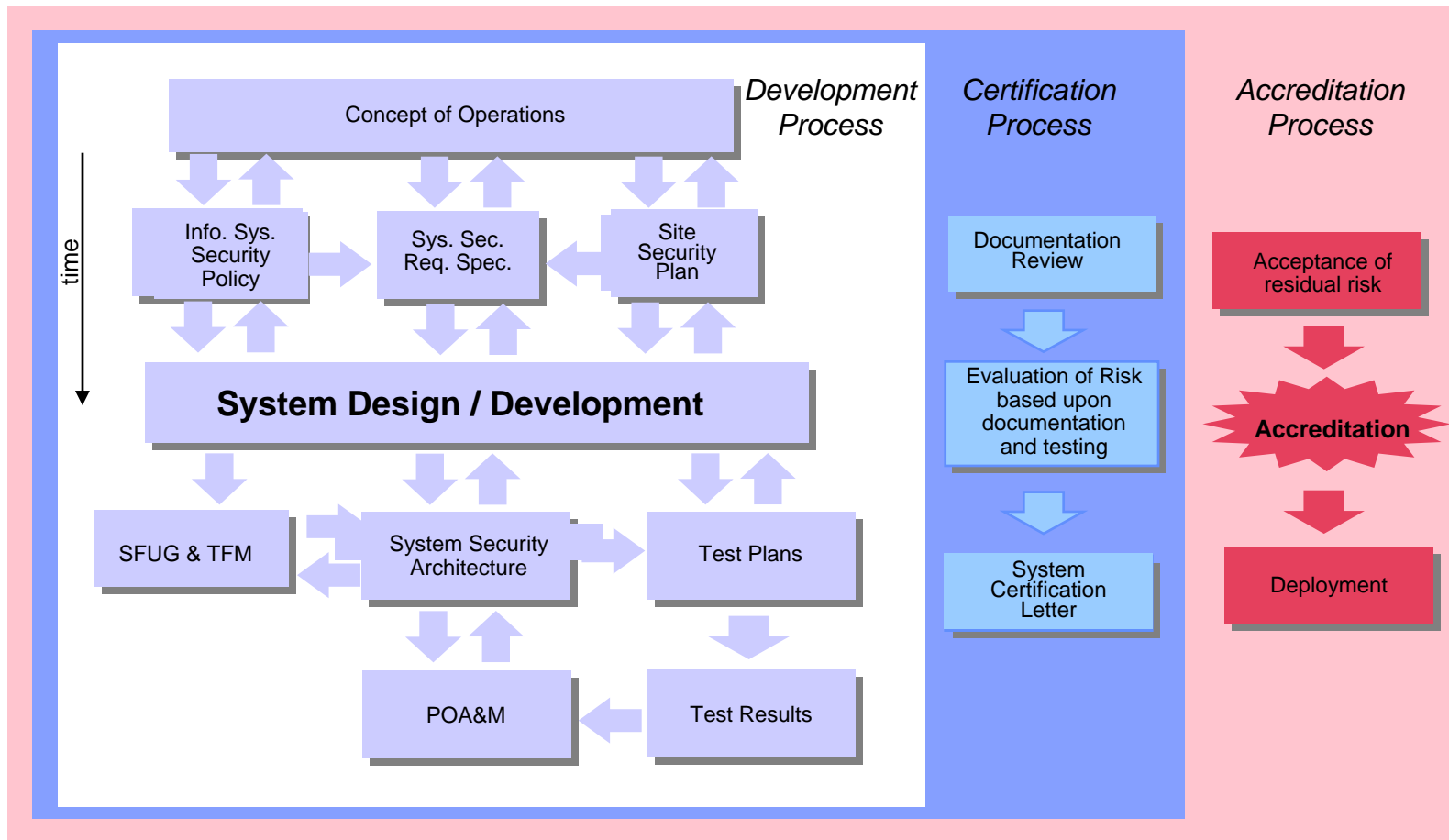
- Update all evidence

C&A Documents



Document	Audience	Purpose
SSAA / SSP	DAA	Executive summary of key information in the appendices.
C&A Plan	DAA, CA, PM, User Rep	Primarily boilerplate, but it identifies the key players (its audience), lays out the typical C&A activities/deliverables/responsibilities, and contains the C&A schedule.
CONOPS	All	First doc written (high-level); identifies mission need & op reqs, describes existing system, identifies its shortcomings, and presents concept to overcome those shortcomings.
Security Policy	DAA, CA, PM	Based on CONOPS, high-level INFOSEC props (typically in gov regs) plus site-spec INFOSEC needs.
Security Reqts Trace Matrix	CA, Testers, PM, Developers	Based on the Security Policy, specific “what” statements (typically found in standards like the Common Criteria) that drive the system design/architecture. The matrix is a mapping between security requirements and test procedures that is filled in as tests are developed to ensure testing is necessary and complete.
Architecture	Developers, Testers	Based on CONOPS and Sec Req, “how” design information that leads to system implementation.
Test Plans & Procedures	CA, Testers	Based on the Security Requirements and the Architecture, the specific tests (e.g., CT&E and ST&E) that verify the system and its environment meet their security objectives.
Test Results & POA&M	CA, PM, Developers	Based on implementation of the Test Procedures, these two documents capture the residual risk of operating the system in its particular environment and the plan for addressing those risks.
Site Security Management Plan	ISSM	Based on the CONOPS, the Security Policy, and the Security Requirements, site-specific procedural information for implementing a secure environment.
Admin Guide	ISSO	Based on the Architecture, technology-specific information for installing, configuring, and maintaining the system.
MOUs/C&A Ltrs	DAA, CA, PM	Official statements from the DAA(s) and CA.

C&A and the Engineering Process

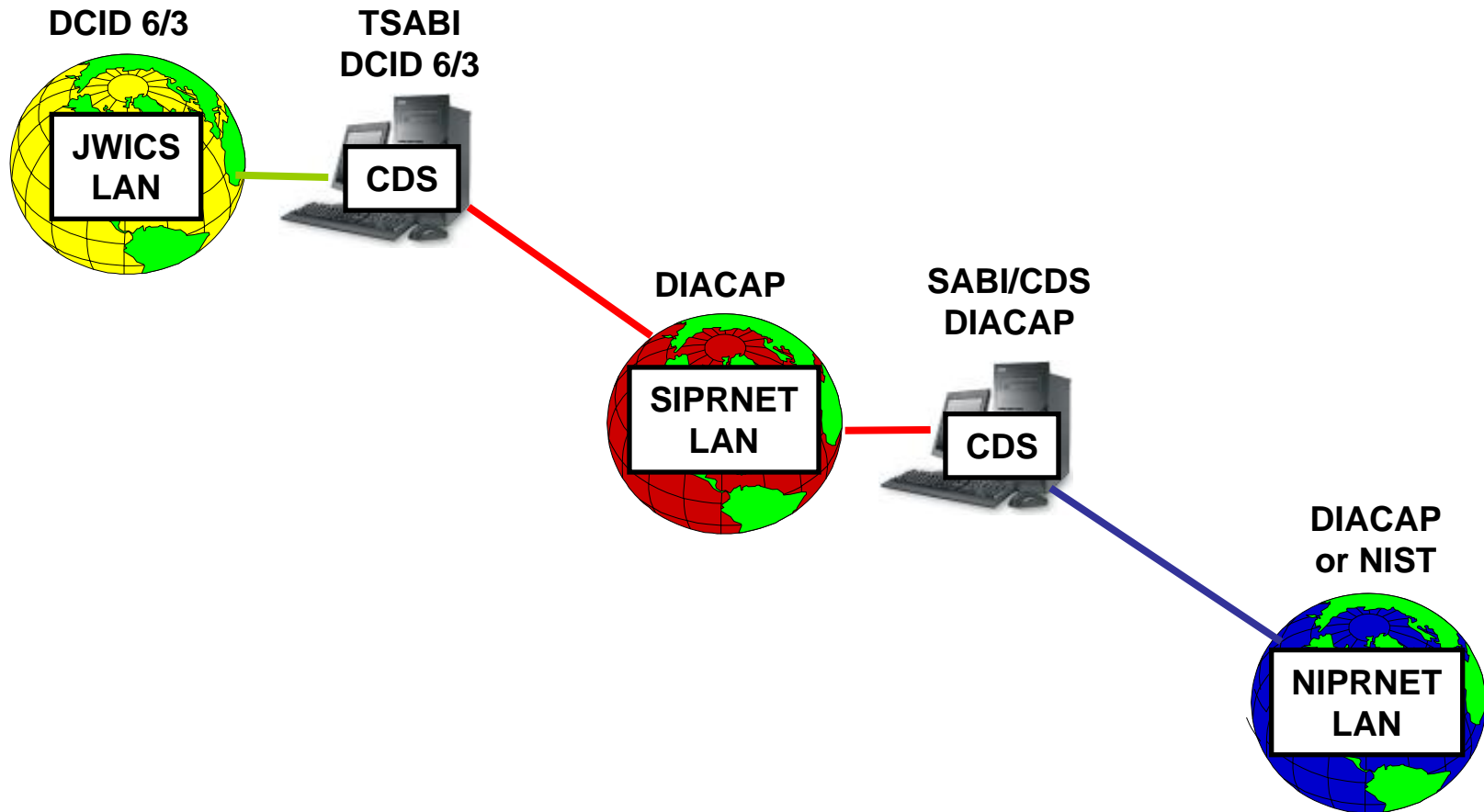


Getting Started with C&A



- Identify the roles (name, phone, fax, email)
- Establish a tentative schedule
- Develop the Concept of Operations
 - Identify the mission
 - State the high-level system requirements/controls
 - Provide a high-level system description/diagram
- Begin gathering information for other documents
 - Site IA policy
 - Site security (e.g., incident response, personnel controls)
 - Detailed architecture

What Do You Need To Be Accredited?



C&A Approaches



- DITSCAP to DIACAP
 - DCID 6/3
 - NIST (based on FISMA)
- } DNI / CNSS

What is DITSCAP?



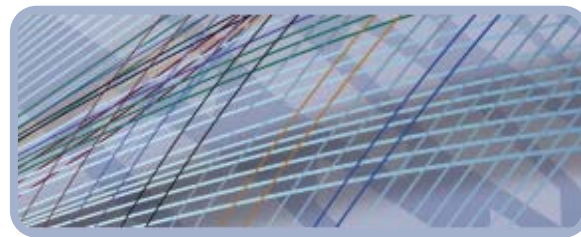
- DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- Developed by DISA (in conjunction with NSA, Services, and Agencies)
- Combination of an instruction and a manual
 - DoDI 5200.40: DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
 - DoD 8510.1-M: Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual

What is DIACAP?



- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Developed by the Office of the Secretary of Defense (OSD)
- DoDI 8510.01: DoD Information Assurance Certification and Accreditation Process (DIACAP) – which is based on
 - DoDI 5200.40
 - DoD 8510.1-M
 - Section 3541 of title 44, United States Code, “Federal Information Security Management Act of 2002” (FISMA)
- Supersedes DoDI 5200.40 and DoD 8510.1-M
- New tools
 - DIACAP Knowledge Service (KS)
 - Enterprise Mission Assurance Support Service (eMASS)

DIACAP Approaches



- DoD
 - DoDI 8510.01
 - Knowledge Service
 - eMASS (interim is IA CAT)
- Army
 - Site DAAs
 - AR 25-2
- Navy
 - In transition from DITSCAP
 - RFI for C&A Support Tool (CAST)
- Air Force
 - High-level DAAs
 - IT Lean Process
 - Security, Interoperability, Sustainability, Supportability and Usability (SISSU)
 - Enterprise Information Technology Data Repository (EITDR)

What is DCID 6/3?



- Director of Central Intelligence Directive (DCID) 6/3
 - ***In process of being replaced by Intelligence Community Directive (ICD) 503***
- Developed by the DCI (in coordination with DISA's DITSCAP)
- Collection of directives, memorandums, etc
 - DCID 6/3: Protecting Sensitive Compartmented Information within Information Systems [directive]
 - DS-2610-142-01: DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide [application]
 - U-3,143/DS-IM: DoDIIS Instructions 2000 [detailed testing and review process]
 - Joint DoDIIS/Cryptologic SCI Information Systems Security Standards [additional/overlapping requirements]

What is NIST C&A?



- Developed by the the National Institute for Standards and Technology (NIST) in response to a legislative mandate in the Federal Information Security Management Act (FISMA) of 2002
- ***Starting point for CNSS publications***
- Collection of Federal Information Processing Standards (FIPSs) and Special Publications (SPs)
 - FIPS Publication 199 (Security Categorization)
 - FIPS Publication 200 (Minimum Security Requirements)
 - NIST Special Publication 800-18, Rev 1 (Security Planning)
 - NIST Special Publication 800-26, Rev 1 (Reporting Formats)
 - NIST Special Publication 800-30 (Risk Management)
 - NIST Special Publication 800-37 (Certification & Accreditation)
 - NIST Special Publication 800-53 (Recommended Security Controls)
 - NIST Special Publication 800-53A (Security Control Assessment)
 - NIST Special Publication 800-59 (National Security Systems)
 - NIST Special Publication 800-60 (Security Category Mapping)

What is the New DNI/CNSS Process?



- Began with C&A Revitalization Effort
 - Kickoff in June 2006
 - DNI, DoD, and NIST initiated development of a new unified approach to C&A
- DNI/CNSS Process
 - New single-level process will apply to all National Security Systems (NSS)
 - The NIST C&A Structure was the starting baseline for this process
 - Will replace DCID 6/3
 - Scheduled to begin 1 Oct 2008
- DIACAP will remain in effect for non-NSS systems

CDS C&A Processes



- SABI/CDS
 - TSABI
- } UCDMO

What is SABI/CDS?



- Cross-Domain Solutions (CDS) – formerly Secret and Below Interoperability (SABI)
- SABI was developed by DISA and NSA, and CDS is a follow-on that is being developed by the Chairman of the Joint Chiefs of Staff
- Roles
 - NSA
 - CDTAB
 - DSAWG
- Activities
 - CT&E (SR 1-9)
 - ST&E
 - Risk Assessment (RDAC)
- Documents
 - Cross Domain Appendix (CDA)

SABI/CDS Roles

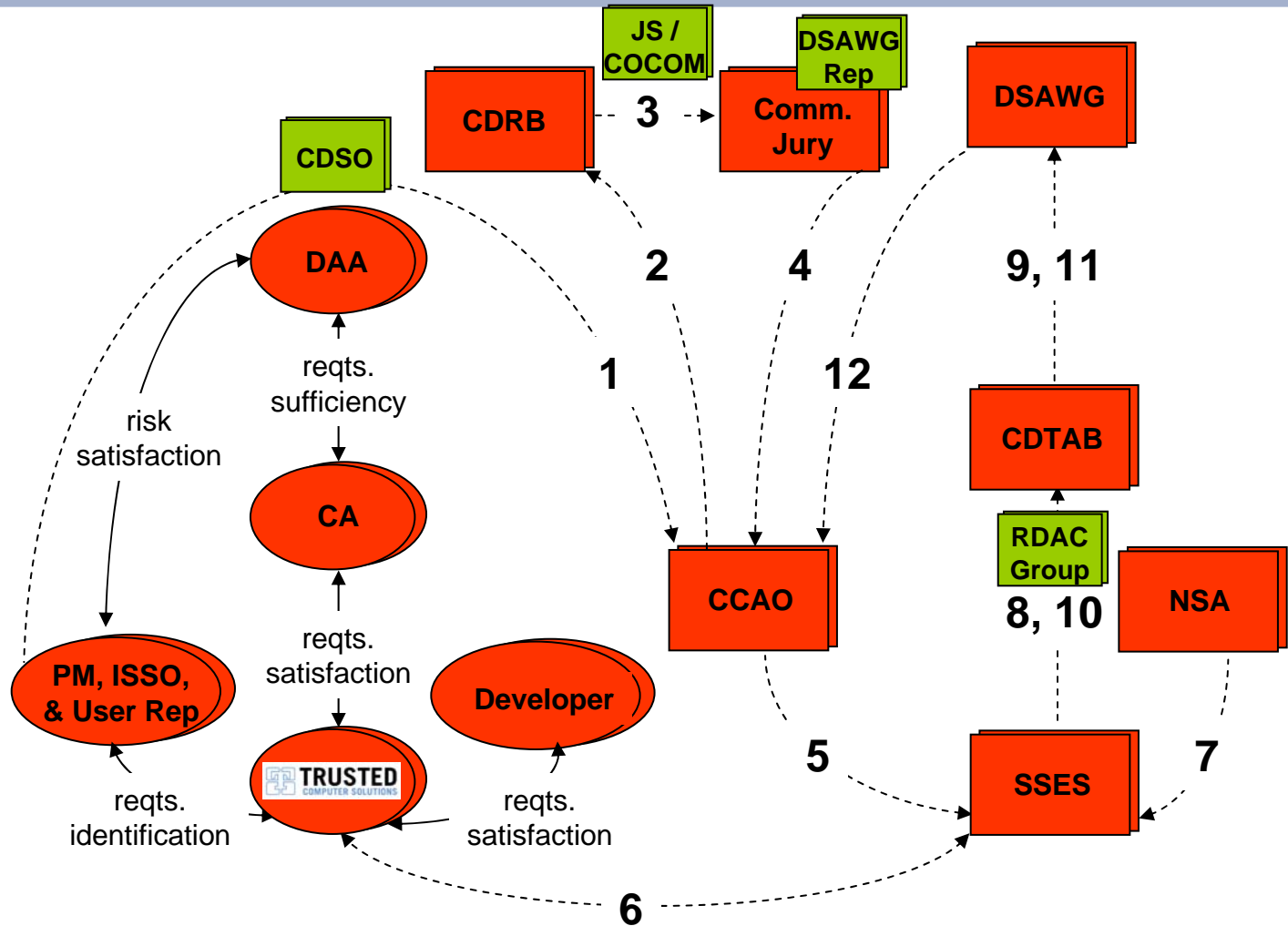


- SABI/CDS Roles

- CCAO
- CDRB
- Comm. Jury
- SSES
- NSA
- CDTAB
- DSAWG

- Newer Roles

- CDSO
- Joint Staff
- RDAC Group
- COCOM
- DSAWG Rep



What is TSABI?



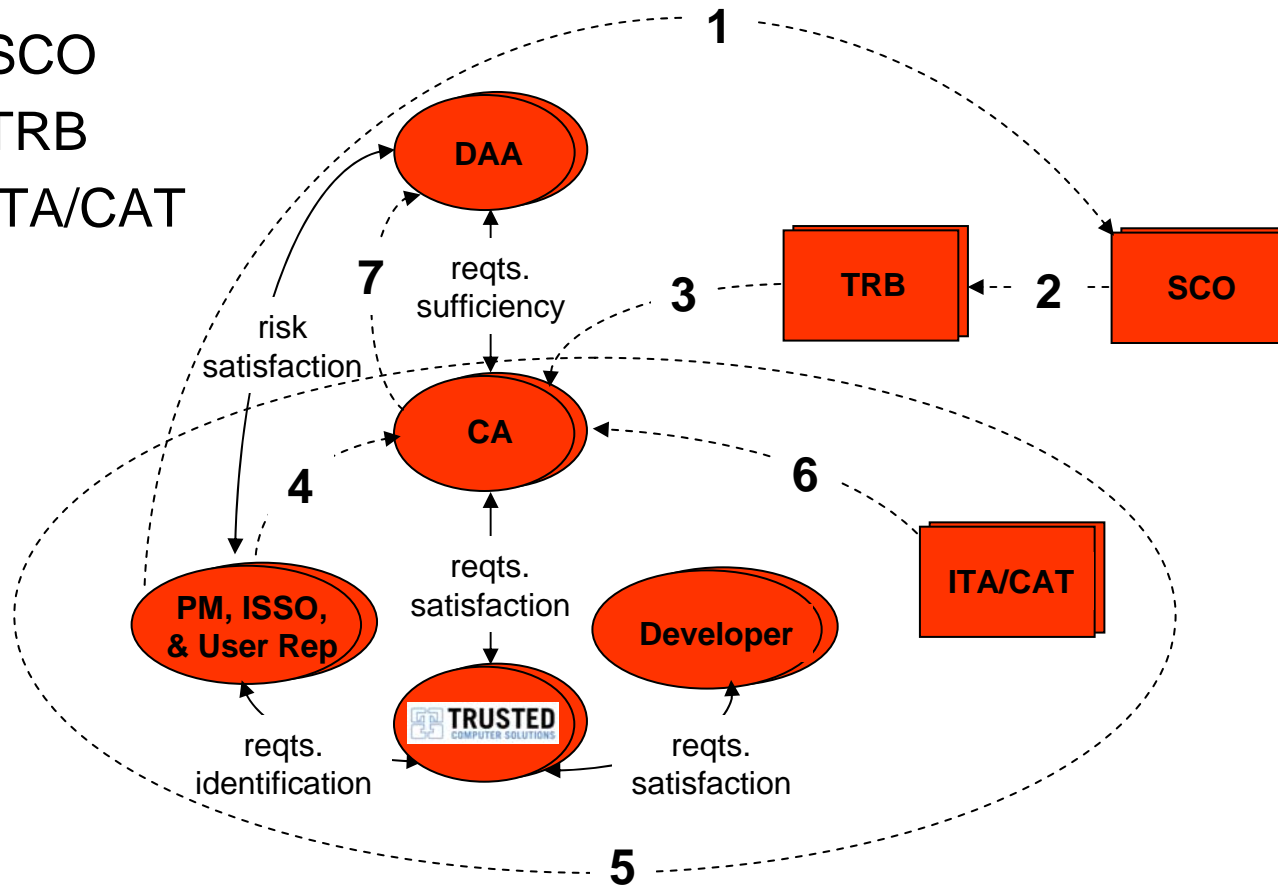
- Top Secret SCI and Below Interoperability (TSABI)
- TSABI was developed by the Intelligence Community (IC)
- Director of Central Intelligence Directive (DCID) 6/3 has been replaced by Intelligence Community Directive (ICD) 503
- Roles
 - DIA
 - PAA
 - ITA / CAT
- Activities
 - Beta I
 - Beta II
- Documents
 - Short Form SSAA / SSP

TSABI Roles



- TSABI Roles

- SCO
- TRB
- ITA/CAT

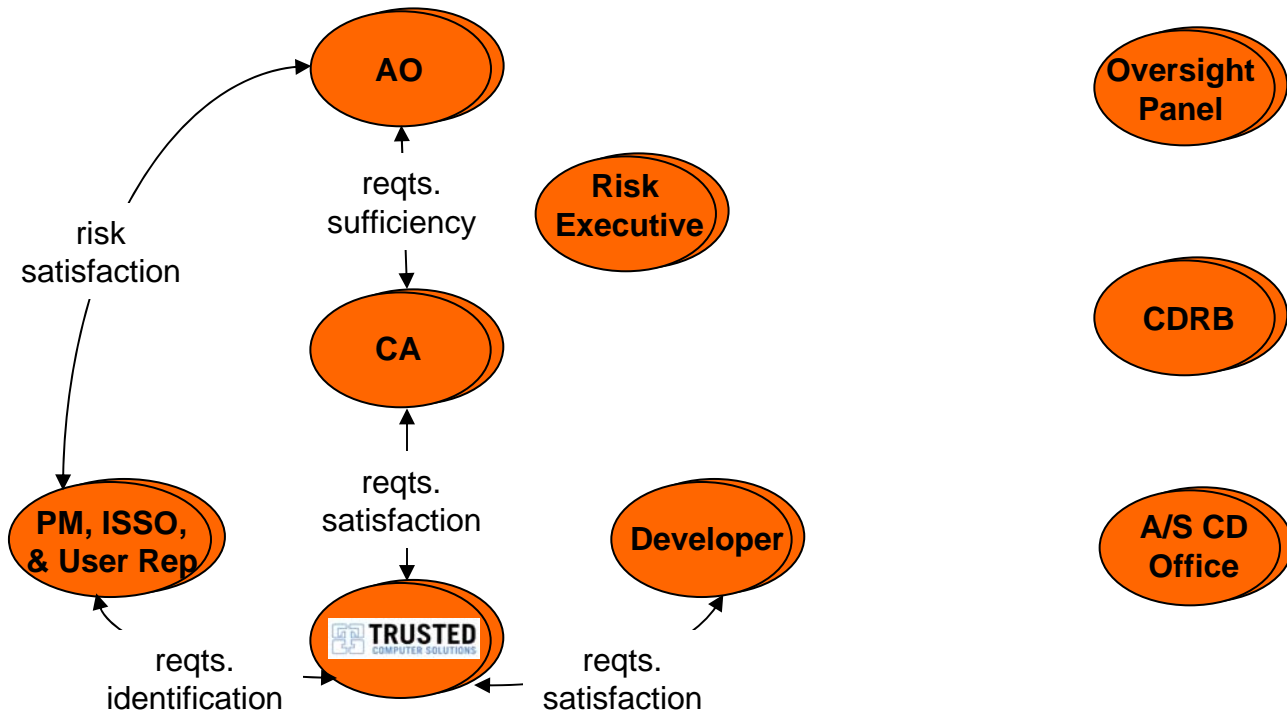


What is the UCDMO?



- Unified Cross Domain Management Office (UCDMO)
 - Established on 10 July 2006 by the DNI CIO and DoD CIO
 - UCDMO pertains to all Intelligence and DoD CDS
- Mission – Provide centralized oversight of all cross domain activities
- C&A for CDSs (DoD & IC) will be conducted using the same processes and standards as other IT solutions
 - C&A process and CNSSI 1253 are beyond UCDMO control
 - UCDMO can and have made comments/suggestions to C&A Team
- UCDMO CD Inventory Lifecycle Stages
 - Research & Development (R&D) List
 - Certification Test & Evaluation (CT&E) List
 - **CD Baseline**
 - Sunset List

UCDMO Roles



Summary



- C&A Principles
 - Roles
 - Activities
 - Documents
- Overview of C&A Approaches
 - DITSCAP to DIACAP
 - DCID 6/3
 - NIST (based on FISMA)

} DNI / CNSS
- Overview of Cross Domain Solution (CDS) C&A Processes
 - SABI/CDS
 - TSABI

} UCDMO

Your Questions Answered



- Let's clarify. Did he say that even if the CDS has undergone a CT&E from another organization that it is still required instead of just the ST&E? This is in the SABI community and not the TSABI.
 - **Lab-based CT&E testing is only required once for a particular version of a product. If the product version changes, a one-time CT&E regression test may be necessary.**
 - **On-site ST&E testing is required for installation of a CDS at every site (after lab-based CT&E has been completed for that version of the CDS).**
- Is there any formal guidance addressing acceptance of one Service/process by another service/organization? Say army cert accepted by AF?
 - **This is a current topic of discussion in a DIACAP working group. Practically, I would present the Army evidence to your AF certifier/accreditor and request reciprocity.**

Your Questions Answered



- Can a CDS receive a type accreditation if all things are equal - the solution and network connections? The case is generally that systems installed in an organization in a different part of the organization, but has the same attributes. Generally the accreditation received for the one part can be the basis for a type accreditation of the system at the other part instead of going through the full process. Essentially say the same Army organization wishes to install the same CDS in another area of the org. Same building but different room.
 - **Type accreditation is a hot buzzword that can mean different things to different people – I appreciate you defining the way it is used in your organization! See the answer to the prior question about CT&E and ST&E. In general, prior C&A approvals should always be introduced when performing subsequent C&A efforts – really helps with the “warm fuzzy” factor. In your case, I would include both rooms in a single ST&E. If you are adding the 2nd CDS at a later time, either a short ST&E or a written statement that all site risks are covered should work.**

Your Questions Answered



- What is the business reason distinguishing between an ATO and ATC?
 - The ATC/ATO scenario is specific to the SABI process. An Authority to Operate (ATO) is issued by local site DAA to allow the CDS to operate at the site. An Authority to Connect (ATC) is issued by the community DAA (i.e., DSAWG) to allow the CDS to connect to SIPRNet. Both are necessary to make sure the site and the community are aware – a defense-in-depth security control, of sorts.
- Will the JAFAN 6/3 and DCID 6/3 be collapsed around October?
 - Joint Air Force, Army, Navy (JAFAN) 6/3 (for the Special Access Program community) is identical to DCID 6/3 (for the Intel community) except that “SCI” is replaced with “SAP.” I would consider these documents identical/collapsed. I have not heard about any effort to combine them in a particular timeframe, but would not be surprised that JAFAN 6/3 will also follow ICD 503, which is replacing DCID 6/3.

Your Questions Answered



- How do I identify my DAA/IAO?
 - The DAA and IAO are very different roles. The DAA approves operation of a system in a particular environment to accomplish a particular mission. The IAO (often a system administrator) is responsible for implementing information assurance at the site so that the DAA has a “warm fuzzy” to approve operation.
 - The DAA is the person who has the authority to approve operation of the system. Sometimes that is the base commander of his/her representative. Sometimes it is a high-level official that is not on-site.
 - The IAO is usually in the IT support organization.
- How do you see the three C&A processes coming together?
 - I see the NIST C&A approach being the basis for all three communities. NIST is already working with DNI and CNSS to incorporate updates. There will still be some difference, given the different threats and data values in the classified world, but the NIST language should be common.

Your Questions Answered



- Can I reuse C&A evidence from another site?
 - See the answer to the prior question about “type accreditation.” Reuse of Site A content at Site B is fine, as long as the Site B personnel understand the content. You cannot point to another site’s effort and say you are done – you have to make sure that the technology, people, processes and procedures are all properly used and understood by your site personnel, as verified by an on-site ST&E test.
- Is the DAA always the ultimate authority on granting approval?
 - In the case of a single-level LAN connecting to a WAN, the answer is yes.
 - In the case of a CDS being added to an already-approved single-level LAN, both the site DAA and the community DAA must grant approval (see the answer to the prior question about ATO and ATC).