



Defense Information Systems Agency

A Combat Support Agency

UNCLASSIFIED

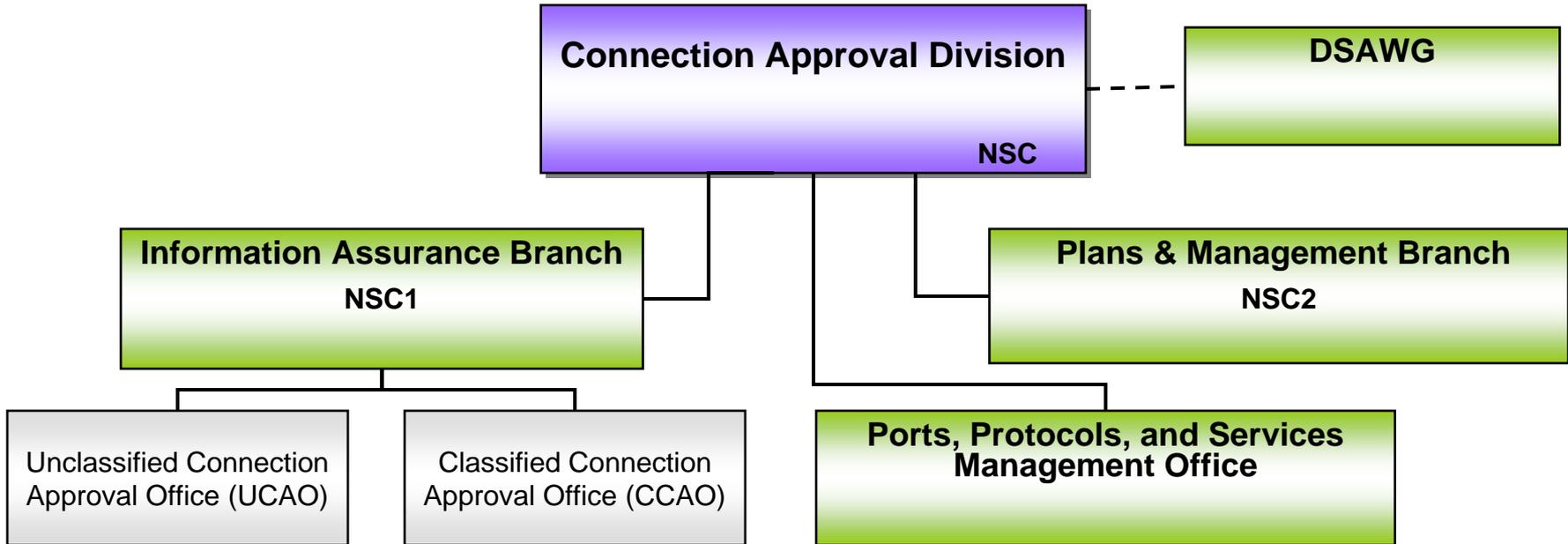
DISN Connection Approval Process (CAP)

5 Feb 09

Overview

- **DISN Connection Approval Division (CAD)**
 - Organization & Mission
 - Functions & Projects
- **DISN Connection Approval Process (CAP)**
 - DoD/CJCS Policy Guidance & DISN/GIG Accreditors
 - Connection Process Goals
 - Connection Process Guide
 - How CAP Works
 - Simplified CAP
 - Risk Assessment Process
 - Cross-Domain Solution (CDS) CAP

CAD Organization & Mission



Mission:

Provide customers a consolidated connection approval process for all DISN services. Information Assurance (IA) manage ports, Internet protocols, and application services for DoD Information Systems. Review and resolve authorization and connection decisions related to the sharing of GIG IA and security risk, as authorized by the DISN/GIG Flag Panel. Approve connections, manage and provide customer-accessible connection and accreditation information, and perform as a Computer Network Defense (CND) partner with CC/S/A.

CAD Functions & Projects

- **Consolidate disparate DISN connection processes into single, common process guide**
- **Modify CAP process to reflect DoD C&A transition from DITSCAP to DIACAP & new CJCS DISN connection guidance**
 - **Includes Cross-Domain Solutions (CDS) & REL DMZ analysis & connection recommendation**
 - **Participate in Enterprise & Centralized CDS process**
- **Manage ports, protocols & services for all DoD IS**
- **Manage customer-accessible IS/enclave connection & registration databases**
 - **Implement federation of SNAP, SGS & PPSM for common look & feel**

DoD Policy Guidance

- **DoDD 8500.01E, Information Assurance (IA), 24 Oct 02 (Certified current as of 23 Apr 07)**
- **DoDI 8500.2, IA Implementation, 06 Feb 03**
 - Basis of IA controls for C&A and connection approvals
 - Requires compliance with DISA FSO STIGs, USSTRATCOM directed solutions (CTOs, FRAGOs, etc.), DoD IAVM Program, NSTISSP 11 (for IA & IA-enabled products), etc.
- **DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 07**
 - DIACAP information “is made available as needed to support an accreditation or other decision such as a connection approval.”
- **DoDI 8100.3, DoD Voice Networks, 16 Jan 04**
 - May be superseded by “Unified Capabilities” DoDI

CJCS Policy Guidance

- **CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities, 09 Jul 08**
 - Establishes policy & responsibilities for connection of IS (e.g., applications, enclaves, or outsourced processes)
 - Applies to Unclas & Class Voice, Video & Data connections
 - Requires IS registry: DITPR (Unclas) & SIPRNet IT Registry (Class)
 - Provides guidance on Cross Domain Solutions (CDS) between security domains
 - Requires CND-SP for all IS/enclaves connected to DISN
 - DISA tasked to develop, maintain & promulgate a customer connection process guide
- **CJCSI 6215.01C, Policy for DoD Voice Networks with Real Time Services (RTS), 09 Nov 07**

Accreditors for DISN/GIG

Local IS/Enclave DAA

Issue Accreditation Decision
Accept Risk to IS/Enclave
Request Connection to DISN

DISN/GIG PAAs

Assess & Accept Risk to DISN/GIG
and All Connected IS / Review
Requests for Special Case Networks /
Final Appeal For CC-level Requests

DISN CAO

Single POC for All
Connection Requests /
Approve Routine, Single-level &
DoD-only Requests

**DISN/GIG
Connection**

DISN/GIG Flag Panel

Approve Policies, Procedures & Standards
on Behalf of DISN/GIG PAAs /
Approve High Risk Connections /
Review Appeals of DSAWG Decisions

DSAWG

Approve Routine Requests /
Preview High-Risk and
Exceptional Requests & Make
Recommendations to Flag Panel

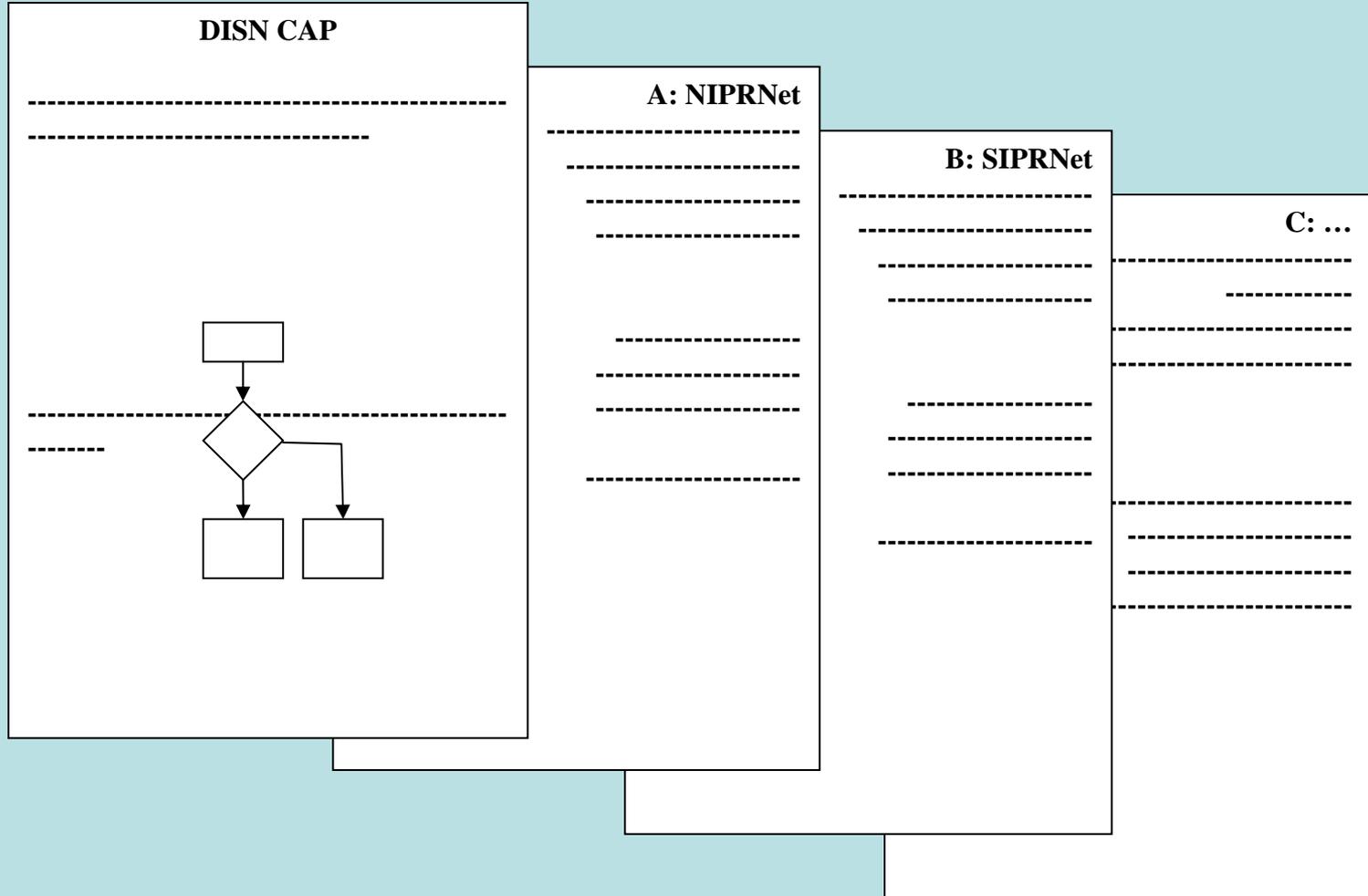
Connection Process Goals

- **Provide a transparent & user-friendly process**
 - Single point-of-entry for customer requirements for connection to all DISN networks/services
 - Site navigation & step-by-step process is clear & concise
 - Streamlined procedures save customer & DISA resources
- **Ensure risk to DISN is measurable & acceptable**
 - Risk assessed at initial & follow-on connection requests
 - Periodic ad hoc assessments provide situational awareness throughout connection life cycle
 - CAO works closely with customer & JTF-GNO when high risk warrants consideration of disconnection from DISN
- **Proper execution of requirements facilitates timely establishment of appropriate connection for mission**

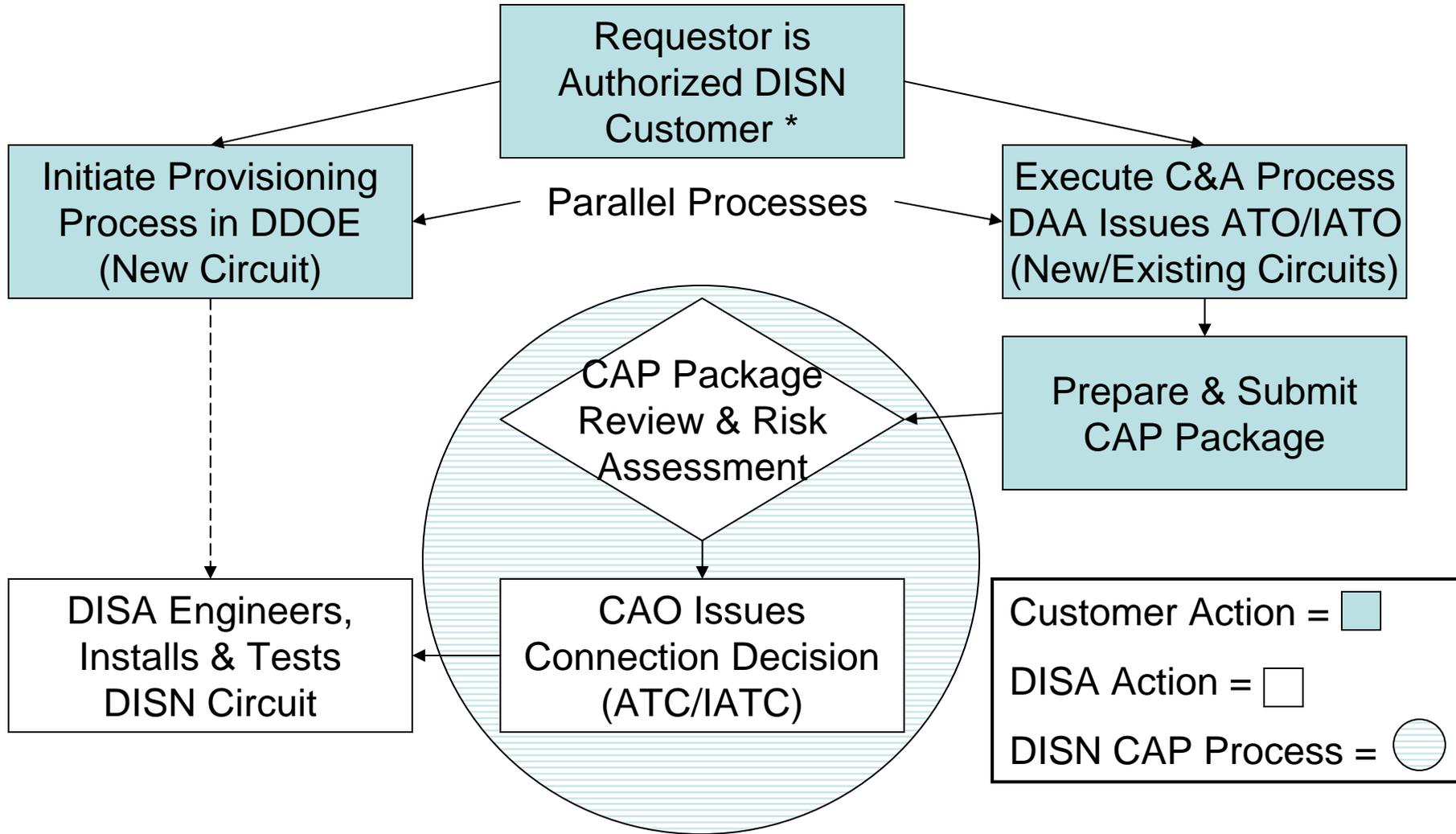
DISN Connection Process Guide

- **Applies to all DoD & Non-DoD customers desiring a connection to any DISN network or service**
 - Must be based on a validated requirement
 - Non-DoD entities require a DoD Sponsor
- **Basic Guide: Requirements & timelines common across all DISN networks & services**
 - NIPRNet, SIPRNet, DSN, DRSN, DVS-II (G), DISN-LES, RTS
 - Examples: DAA Appointment Letter, DIACAP Executive Package, Topology Diagram & Consent to Monitor (CTM)
- **Appendices: Requirements & timelines unique to individual DISN networks & services**
 - Examples: SNAP registration for NIPRNet, SCQ for SIPRNet, APL for DSN/DRSN equipment/software, etc.

DISN Connection Process Guide

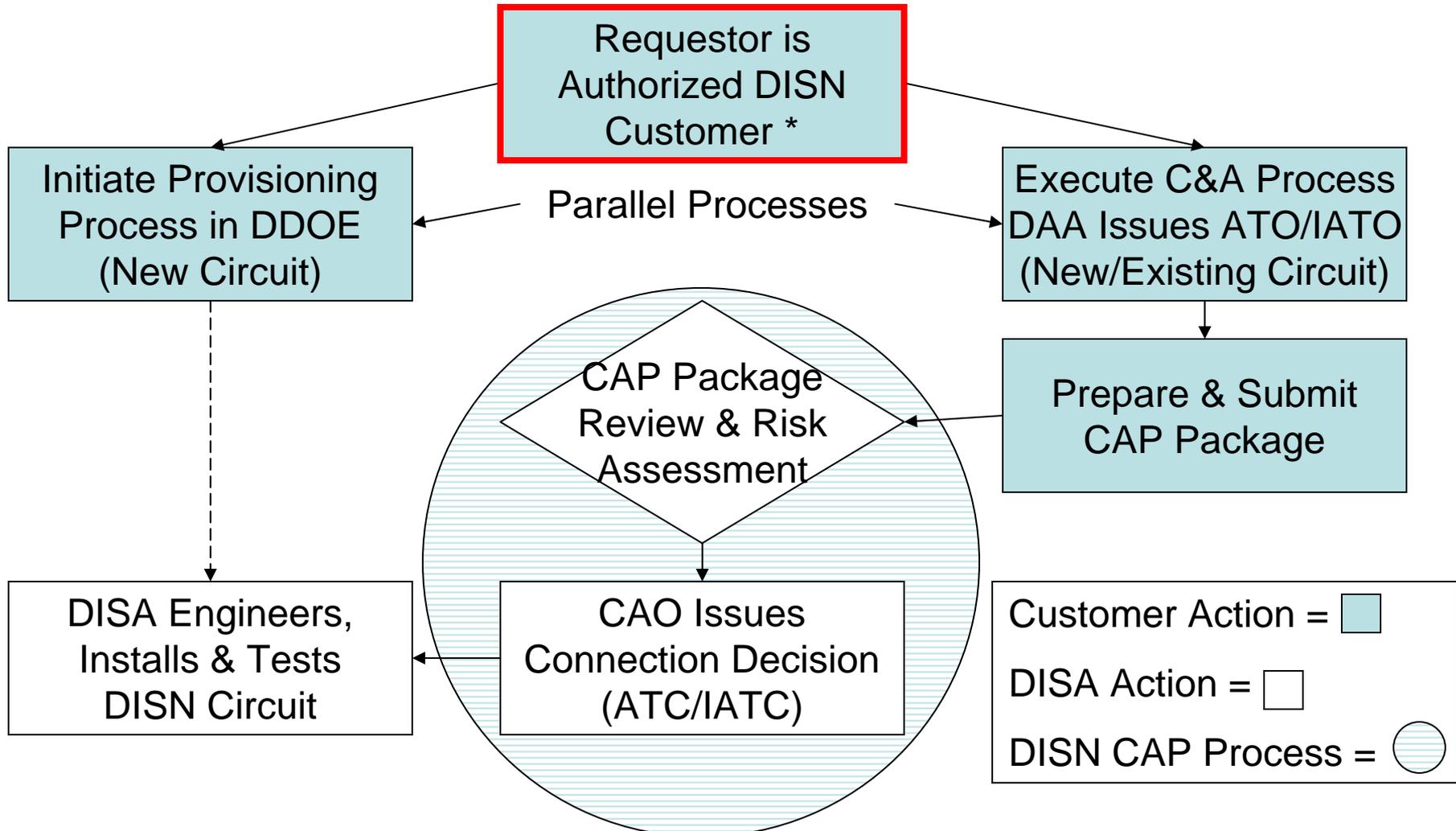


How CAP Works (Simplified)



* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

Customer/Requestor Status

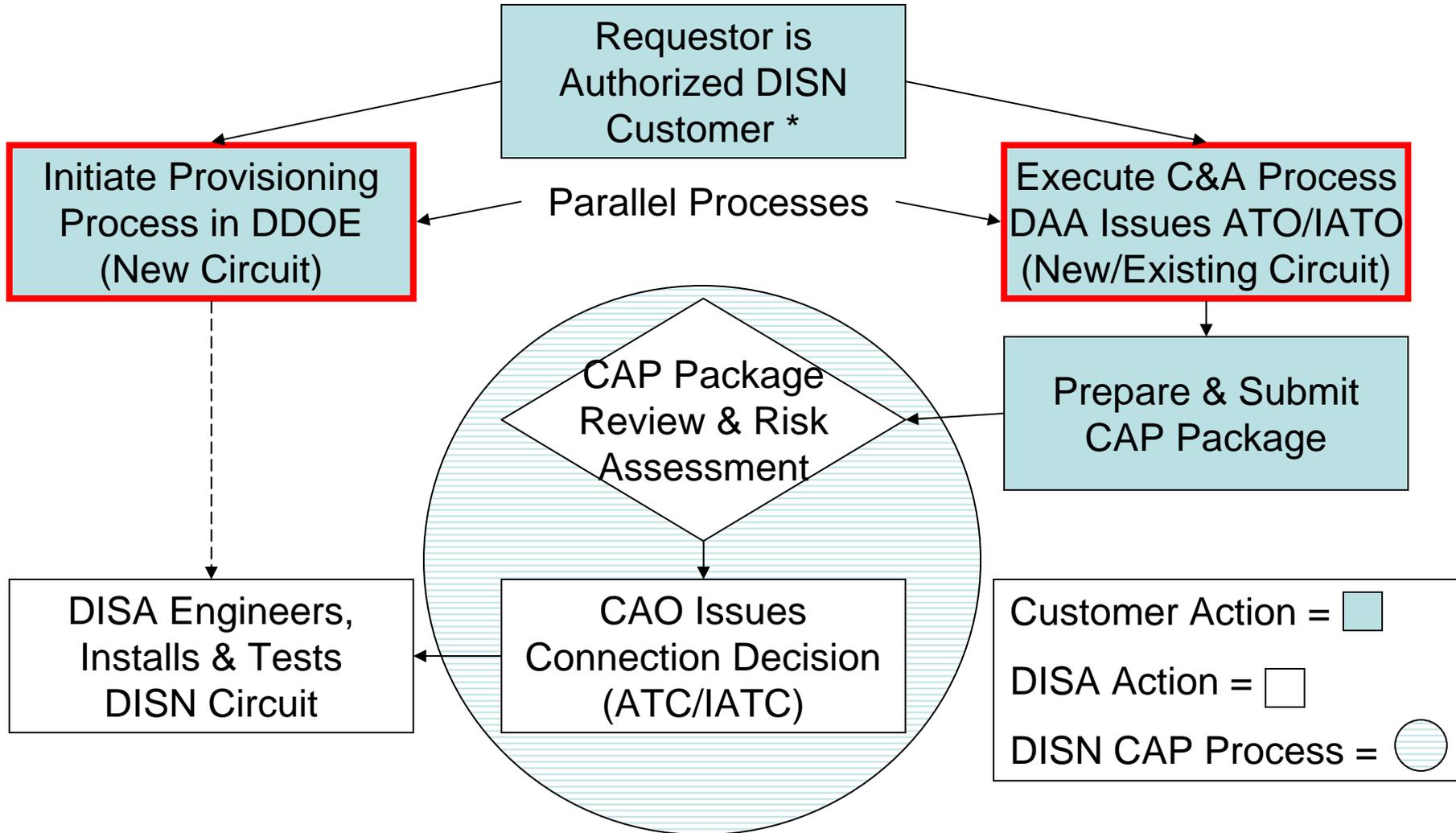


* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

Customer/Requestor Status

- **Customer may be DoD entity or Non-DoD entity**
 - DoD entity requests own connection
 - DoD Sponsor requests Non-DoD connection (for contractors, Federal Agencies, etc.)
 - DISA Customer Call Center (DCCC, 1-800-554-3476) guides customer through network/service selection process
- **Non-DoD mission must be approved by OASD(NII)**
 - Sponsor completes request letter & forwards to CC/S/A
 - Letter includes mission, verification of funding & contract (as applicable), conceptual network topology & other required info
 - CC/S/A validates mission & forwards to DISN Service Manager
 - Service Manager evaluates proposed solution & forwards with recommendation to Sponsor
 - Sponsor submits request to OASD(NII) for approval
 - OASD(NII) acts on request & returns with decision to Sponsor
 - If approved by OASD(NII), Sponsor may begin the DISA Direct Order Entry (DDOE) process

Provisioning and C&A



* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

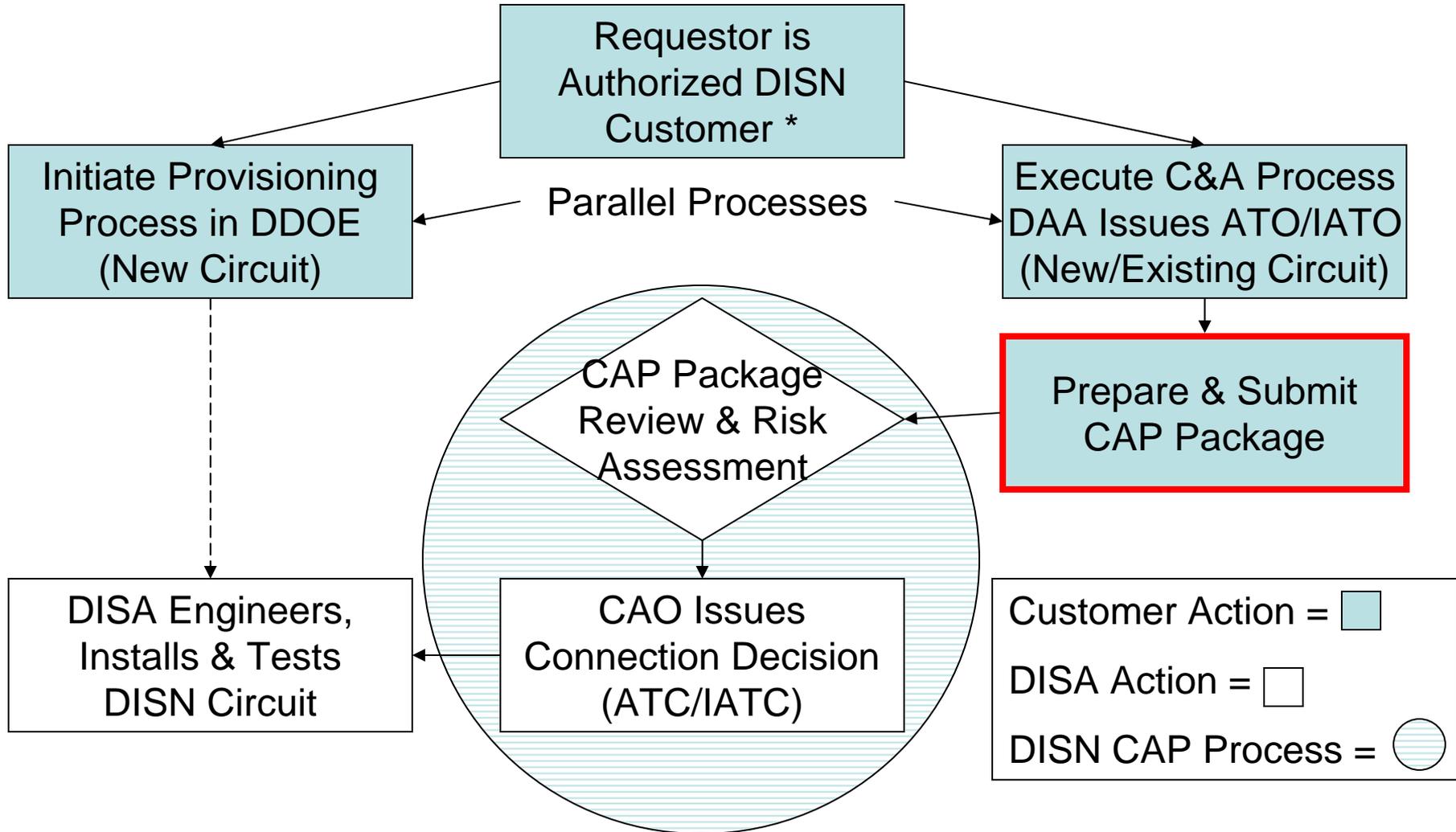
Provisioning and C&A

- After appropriate network/service is identified & any necessary approvals are received, DoD customer (or DoD Sponsor) initiates DDOE process at:
<https://www.disadirect.disa.mil/products/asp/welcome.asp>
- Prior to or in parallel with DDOE process, customer executes C&A process
 - For DoD IS requiring DoD connection to DISN, use DIACAP
 - DoD IS requiring contractor connection to DISN:
 - For UNCLAS connection, use DIACAP (DoD Sponsor is DAA)
 - For CLASSIFIED connection, use NISPOM (DSS is DAA)
 - For Intel Community IS, use ICD 503
 - For Federal Agency IS, use NIST SP 800-37
 - For other Non-DoD entities, C&A process requirements reviewed case-by-case

DIACAP Accreditation Decisions

- **Authorization to Operate (ATO)**
 - Authorization Termination Date (ATD) not to exceed 3 yrs
- **Interim ATO**
 - ATD not to exceed 180 days (change from DITSCAP)
 - Manage IA weaknesses during new system operation
 - Consecutive past 360 days needs Component CIO approval
- **Interim Authorization to Test (IATT)**
 - Only for testing in operational environment or with live data for specified period (ATO/IATO still required for connection)
 - Cannot be used in lieu of (i.e., to avoid) ATO/IATO
 - Not same as the DISA IATT issued to test new DISN circuit
- **Denial of ATO (DATO)**
 - DAA concludes IS should cease operations due to IA issues

Connection Approval Package



* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

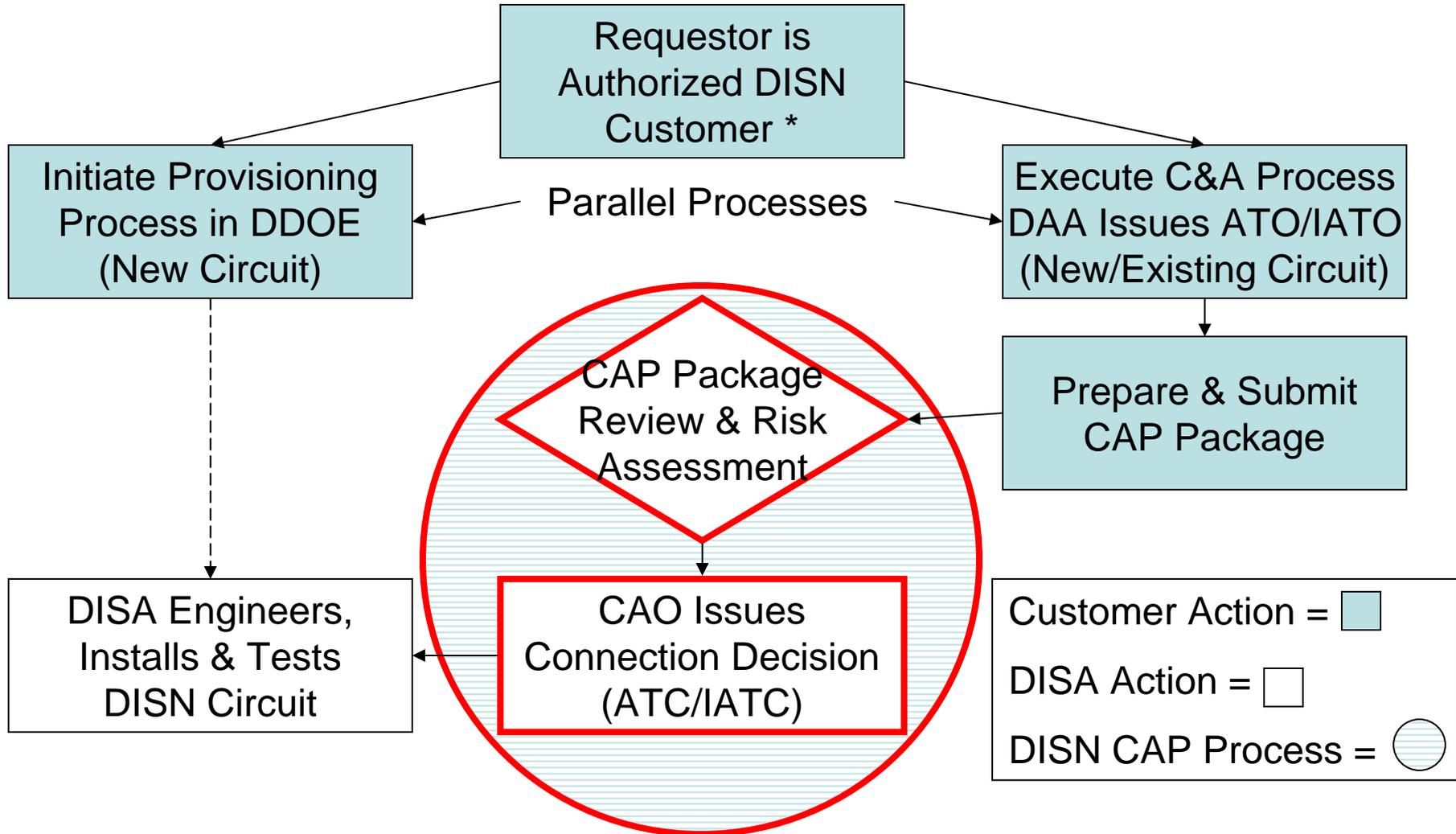
Connection Approval Package

- **For UNCLAS connections submit to Unclassified Connection Approval Office (UCAO) & for CLASSIFIED connections submit to Classified Connection Approval Office (CCAO)**
- **Copy of DAA appointment orders/letter**
 - **Written accreditation approval authority if delegated**
- **DIACAP Executive Package**
 - **Minimum required for accreditation & connection decisions**
 - **DIACAP Scorecard, System Identification Profile (SIP) & IT Plan of Action & Milestones (POA&M)**
 - **Or Equivalent for certain Non-DoD entities**
- **Detailed network topology diagram**
 - **All systems/devices w/ IP addresses, enclave boundary & any/all interconnections to other IS (enclaves, etc.)**
- **Consent to monitor (CTM)**
 - **Allows DISA to conduct on-site and/or remote assessments**

Connection Approval Package

- **Special Cases**
 - **Exercise Connection**: In addition to standard DISN connection requirements, the CC/S/A or field activity headquarters will endorse the connection requirement for exercises
 - **Contingency Connection**: Requesting CC/S/A or field activity organization will submit at least:
 - ATO or IATO issued by the CC/S/A or field activity DAA
 - Interim enclave topology diagram & changes as needed
 - CTM
 - For SIPRNet, a complete & accurate SIPRNet Connection Questionnaire (SCQ)
 - Identification of any Cross-Domain Solution (CDS)
 - Forward completed package to DISA via Combatant Commander's J-6 validation & endorsement process
- **Additional connection-specific elements, which may differ depending on requested network/service**
 - Details in DISN Connection Process Guide

DISN CAP Process



* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

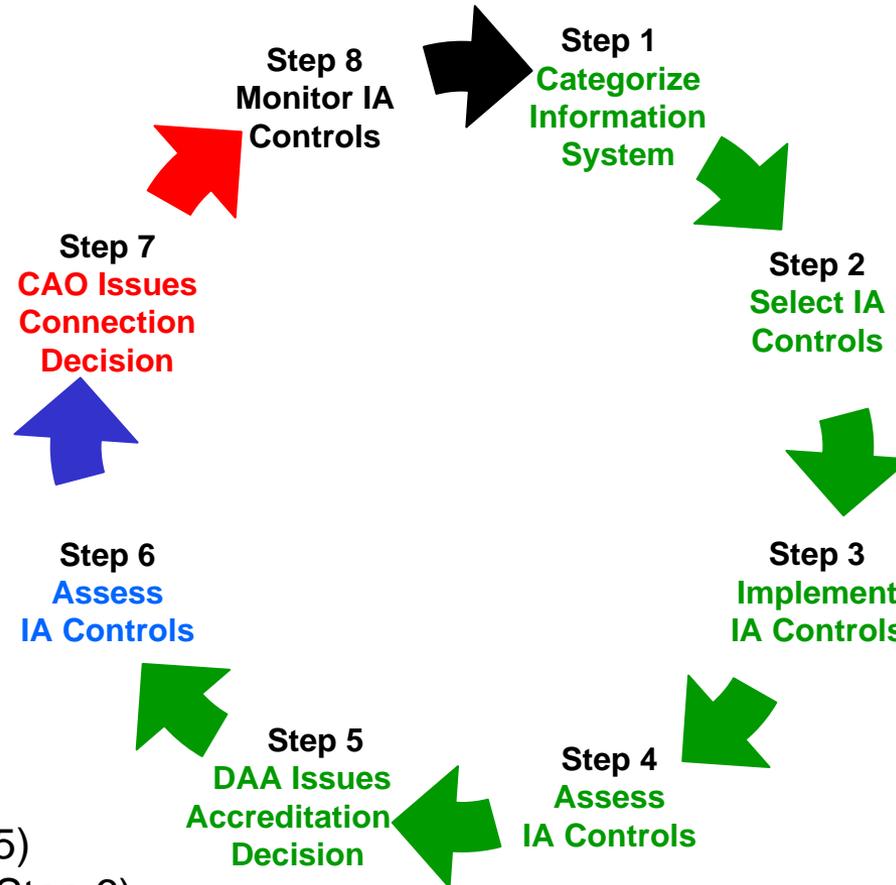
CAP Package Review

- **CAP package submitted to CAO for adjudication**
 - If all requirements are met within required timelines, a new request or follow-on for an existing connection can normally be approved out to the ATD of the ATO/IATO
 - Connection approval decision issued as ATC or IATC
- **Risk posed to the network/service & DISN at large is assessed as integral step in connection process**
 - Assessments will be based on a straightforward methodology & transparent rules that consider all inputs
 - High risk will result in withholding (for new requests) or denial (for existing connections) of approval to connect
- **DAA must remain engaged to ensure IS/enclave compliance with documentation & IA requirements**

CAP Package Review

- **Most delays in issuing ATC/IATC are due to customer-side lag in meeting requirements**
 - **CAO must have complete & accurate information to process request & assess risk**
 - **ATO/IATO often allowed to expire – connection approval must be denied if accreditation decision no longer valid**
 - **IA issues often allowed to go uncorrected, causing high risk**
 - **All IS require registration / inclusion in appropriate DISN database:**
 - **PPSM for all IP IS**
 - **DITPR (for UNCLAS) & SIPRNet IT Registry (for CLASSIFIED)**
 - **SNAP for all UNCLAS IS & SGS for CLASSIFIED IS**
- **IS/enclave POC contact information often outdated**
 - **DAA, Tech & Admin POCs & DoD Sponsor (if applicable)**
 - **NIPRNet & SIPRNet (if applicable) email & Tel/Fax numbers**
 - **If we can't reach you, we can't resolve issues = potential high risk**

CAP Risk Management Framework



Legend:

DAA Action (Steps 1-5)

CAO & DAA Action (Step 6)

CAO (and in some instances DSAWG) Action (Step 7)

DAA, CC/S/A, CAO, FSO & JTF-GNO Action (Step 8)

Risk Assessment Process

- **Identify IA noncompliance issues that increase risk**
 - Missing or inaccurate/incomplete CAP package input
 - FSO ECV, CAO remote scans & enclave self-assessments
 - JTF-GNO IAVM program & network mapping scans
 - IAM annual review of all & test of selected IA controls
 - Other outside agencies (e.g., DoD IG, GAO, etc.) may also periodically assess IA controls
- **Measure responsiveness of enclave in correcting validated weaknesses**
 - Remediation / mitigation requirements & timelines IAW DIACAP, IAVM Program & DISN Connection Process Guide
 - CAO works with customer & others to resolve issues

DIACAP Requirements

- **CAT I Weakness**
 - Must be corrected before new ATO is granted
 - Existing ATO/IATO - CAT I must be corrected within 30 days
 - Include/keep in POA&M, even after corrected/mitigated
- **CAT II Weakness**
 - New ATO may be granted when CAT II weaknesses are present, but only when there is clear evidence that they can be corrected or satisfactorily mitigated within 180 days
 - Existing ATO/IATO - CAT II must be corrected within 90 days
 - Include/keep in POA&M, even after corrected/mitigated
- **CAT III Weakness**
 - DAA may accept risk
 - Include/keep in POA&M, even after corrected/mitigated
- **DIACAP & FISMA require annual IAM review of all & testing of selected IA controls - report to CA & DAA**

CAO Role & Risk Assessment

- **CAO is not the C&A “Cop”**
 - CC/S/A are responsible for IS/enclave C&A enforcement
 - CAO implements DoD, CJCS & DISA connection policies
 - CAO provides high risk assessments to DSAWG & JTF-GNO
- **High Risk = withholding of new connection or denial of approval to connect (DATC) for existing circuit**
 - Usually includes ID & validation of CAT I vulnerabilities
 - CAO notifies DAA of status with rationale & works with customer to remediate or mitigate vulnerabilities
 - If risk can not be downgraded, action forwarded to DSAWG (for existing connections only)
- **Medium Risk = closely monitor IA status**
 - Incomplete or inaccurate CAP Package will cause delay in risk assessment & connection decision processing
 - CAO may request additional information to verify IA status
- **Low Risk = no negative impact**

High Risk / DATC Procedures

- **CAO works with customer to resolve issues**
- **Customer has 30 days to validate & fix CAT I weaknesses and/or other high-risk issues**
 - **If CAT I and/or other high-risk issues cannot be corrected, mitigation options may be available (POA&M required)**
 - **If customer rejects validity of some findings, CAO will evaluate customer evidence & may reassess risk**
- **When customer confirms correction/mitigation, CAO verifies w/ available means within 10 days**
 - **If correction/mitigation confirmed, connection approval process continues normal course**
- **If high risk remains, DATC recommendation sent to DSAWG, cc: DAA, CC/S/A, DoD Sponsor (if applicable)**

Post-DATC Actions

- **If DSAWG approves DATC, CAO forwards to JTF-GNO**
- **JTF-GNO initiates disconnect review procedures**
 - **Assesses (w/ CC/S/A) operational impact of disconnect**
 - **Issues a USSTRATCOM order for immediate disconnect if severe noncompliance issues warrant**
 - **If less severe, releases message giving customer 30 days to bring connection into compliance, or submit a plan to achieve compliance within 60 days of message release**
 - **Issues a coordinated USSTRATCOM order to disconnect if compliance is not achieved within 30- or 60-day windows**
- **Circuit remains in DATC status until brought into compliance or disconnected**

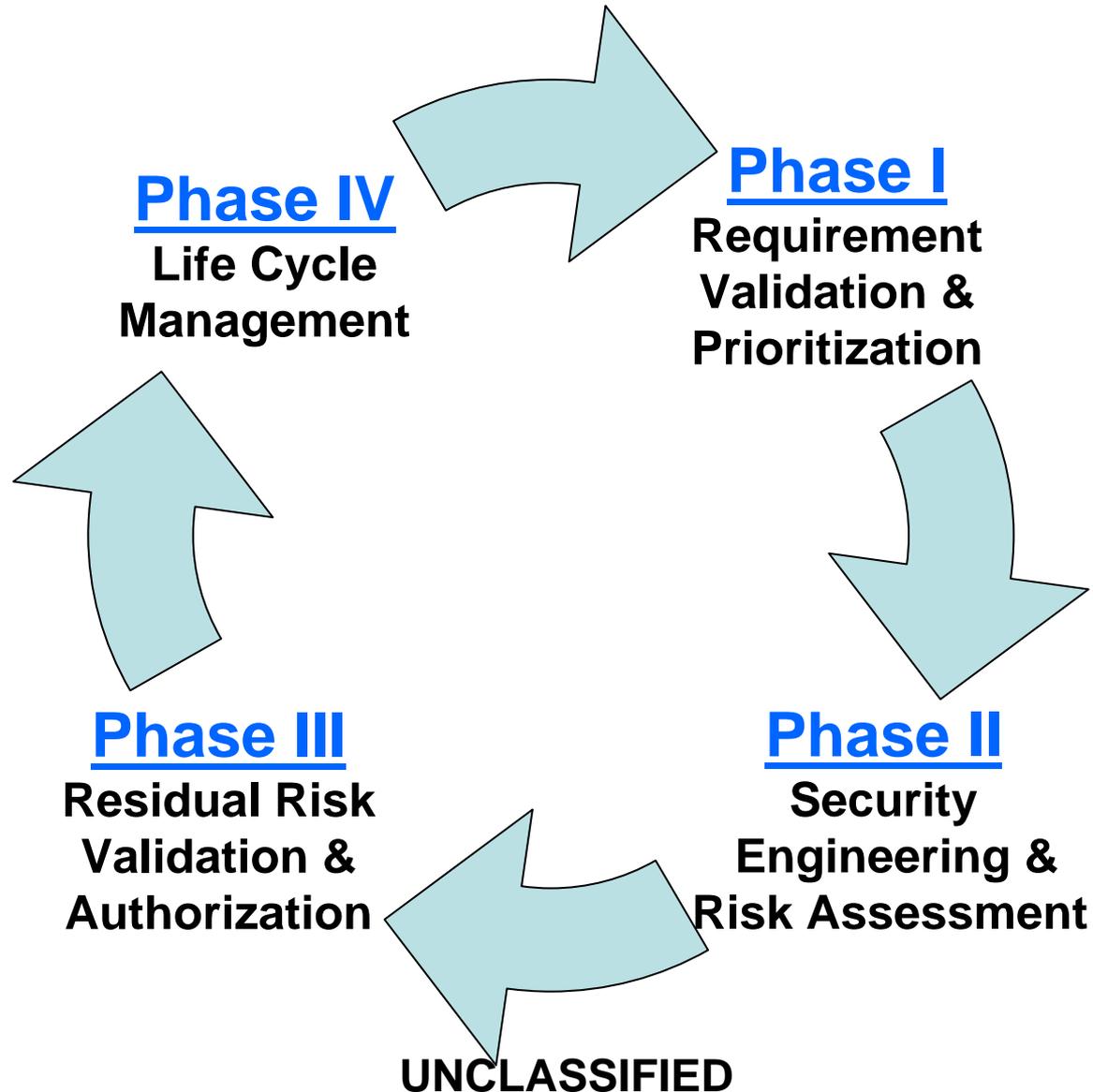
CDS CAP Process

- **Cross-Domain Solutions (CDS) (aka, “guards”) are special cases for connection approval**
- **Enclaves w/ CDS connection requirement**
 - NIPRNet–SIPRNet, SIPRNet–REL, SIPRNet–TS
- **UCDMO, NSA & DISA work together on CDS requests & tickets**
- **DSAWG authorizes connection period of max. 1 yr**
- **IAW CJCSI 6211.02C, DAA must:**
 - Submit to CAO results of the annual security review
 - Include CDS info in enclave accreditation & topology
 - Inform CAO (via signed memo) when a CDS is no longer required or is disconnected

CDS CAP Process

- **Before opening a request, customer must document information transfer & protection requirements**
- **IAW CJCSI 6211.02C, documentation will include:**
 - **Operational requirements**
 - **Information types & classifications**
 - **Type of user access required**
 - **Applicable policy (e.g., security classification guidance for classified information, FOIA exempted information protection guidance and/ or Privacy Act information protection requirements)**
 - **Characterization of threats to the information types & classifications (type & characterization of adversaries, adversary attack types & motivations)**

CDS CAP Process Phases



CDS CAP Process Phases

Phase I

Requirements Validation & Prioritization

Customer Identifies Requirements & Submits Request

CC/S/A Validates & Prioritizes Request

CAO Reviews Request & Forwards

CDTAB & DSAWG Preliminary Review & Approval

CDS Ticket

Phase II

Security Engineering & Risk Assessment

Technical Evaluation

Solution Development

CDTAB & DSAWG Review & Recommendation

Authorization to Connect for ST&E

Phase III

Residual Risk Validation & Authorization

NSA ST&E Tech Review, CDTAB Recommendation & DSAWG Authorization

Customer Submits Enclave Accreditation Decision (incl. CDS)

CAO Reviews CAP Pkg & Issues DISN Connection Decision

ATC/IATC (Max 1 year)

Phase IV

Life Cycle Management

Customer Solution Operational

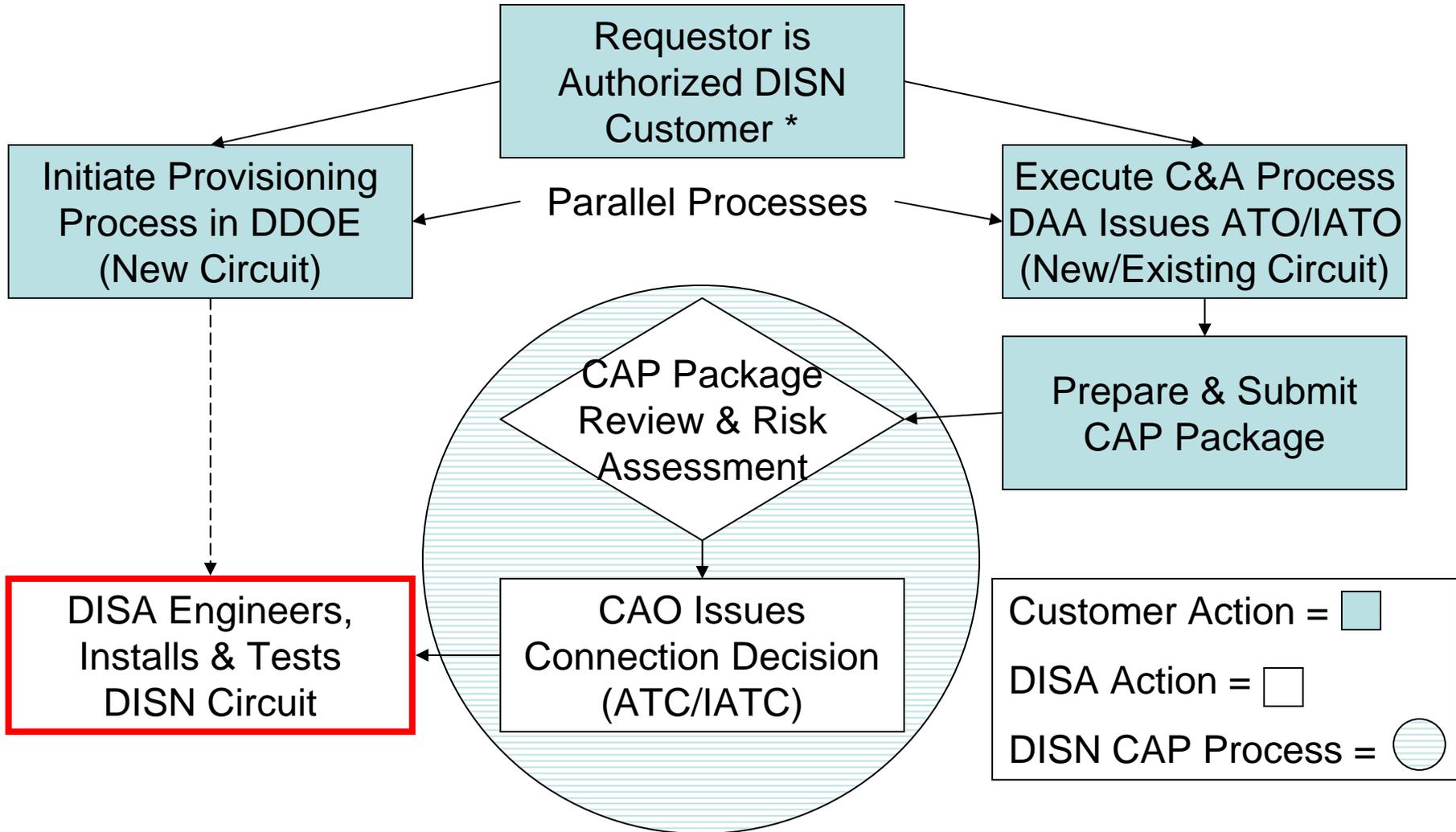
Accreditation Expiration or Major Change

Legend:

Customer Responsibility =

Primarily Other's Responsibility =

Circuit Install & Test



* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

Points of Contact

- **DISN Connection Approval Division**
 - 703-882-0326 (Chief)
- **DSAWG Secretariat**
 - 703-882-0206
- **Classified Connection Approval Office (CCAO)**
 - 703-882-1455
- **Unclassified Connection Approval Office (UCAO)**
 - 703-882-2086
- **Ports, Protocols, and Services Management Office (PPSM)**
 - 703-882-1776
- **DSN for All: 312-381-xxxx**

Questions?

