



**Defense Information Systems Agency**

Department of Defense

# **DISN CONNECTION APPROVAL**

---

**Teri C. Netter**  
**Chief, DISN Connection Approval Division**  
**703-882-0326 (DSN 381)**  
**[teri.netter@disa.mil](mailto:teri.netter@disa.mil)**

Overall Classification of this briefing is:  
Unclassified

**May 2008**



# Connection Approval Division

---

- Division activated 21 Jan 2008

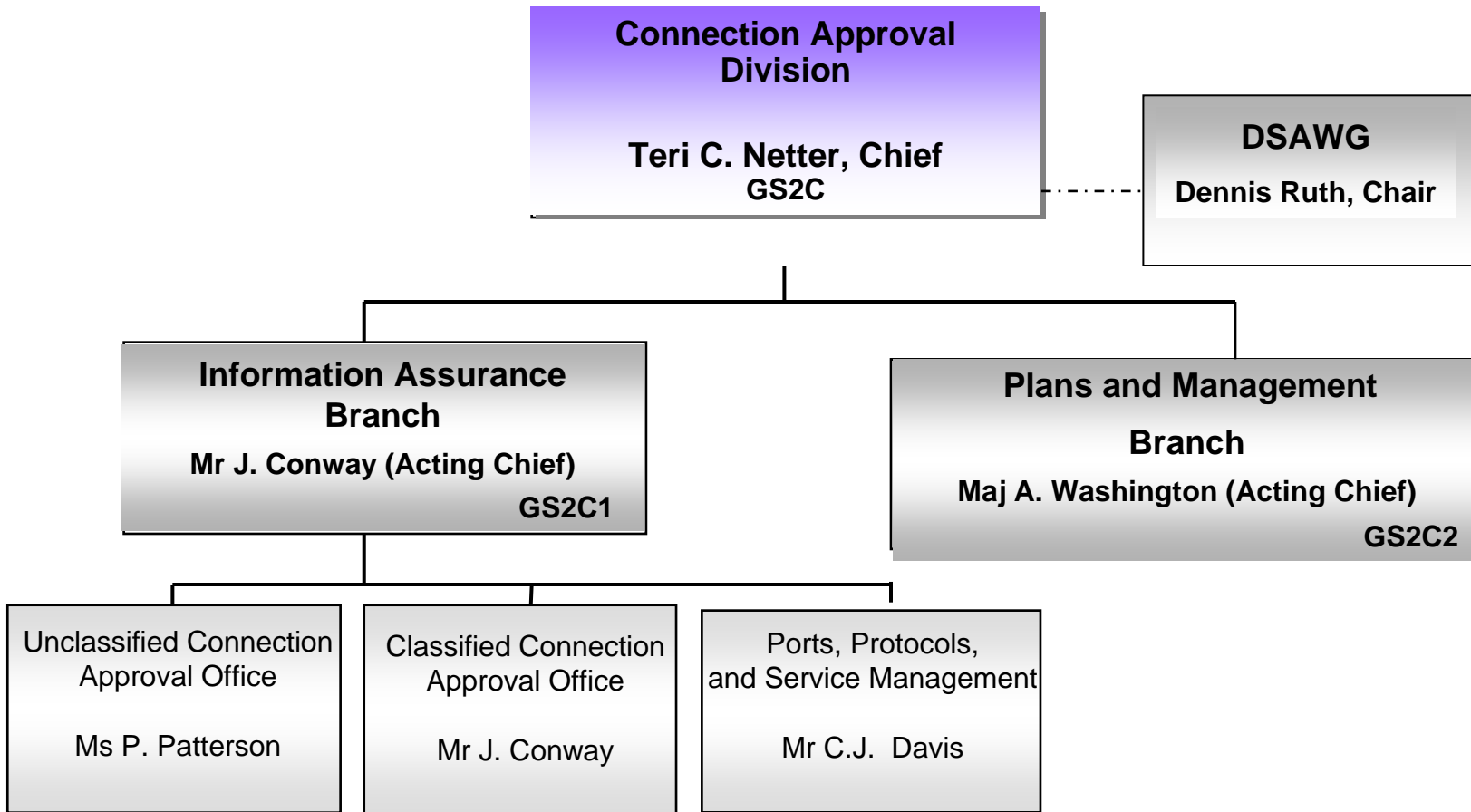
## Mission

Establish and manage a common Connection Approval Process for all DISN services that satisfies Federal, DoD, and JS Information Assurance, interoperability, and connectivity directives. Maintain a user-accessible consolidated database of DISN circuit connection and accreditation status information. Provide Information Assurance management of Ports, Protocols, and Services Management (PPSM) and maintain PPSM registry for all systems connected to the DISN. Chair Defense IA Security Accreditation Working Group (DSAWG), recommend action on all cross domain connections, and make connection approval recommendations to the GIG Flag Panel and DISN DAAs.

**Unclassified**



# Connection Approval Division



Unclassified



---

# **DSAWG – Defense IA Security Accreditation Working Group**

**Unclassified**

# Defense IA Security Accreditation Working Group (DSAWG) Charter

## Policy

- DoDD 8500.1, *Information Assurance (IA)*, October 24, 2002
  - 4.13. All DoD information systems shall be certified and accredited.
  - 4.14. All interconnections of DoD information system shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities to interconnected systems.
    - 4.14.2. Connection to the DISN shall comply with connection approval procedures and processes, as established.

## Authority

- DoDI 8510.01, *DoD Certification & Accreditation Process Guidance (DIACAP)*, 28 November 2007
- CJCSI 6211.02B, Chairman, Joint Chiefs of Staff Instruction, *Defense Information System Network (DISN): Policy, Responsibility and Processes*, 31 July 2003

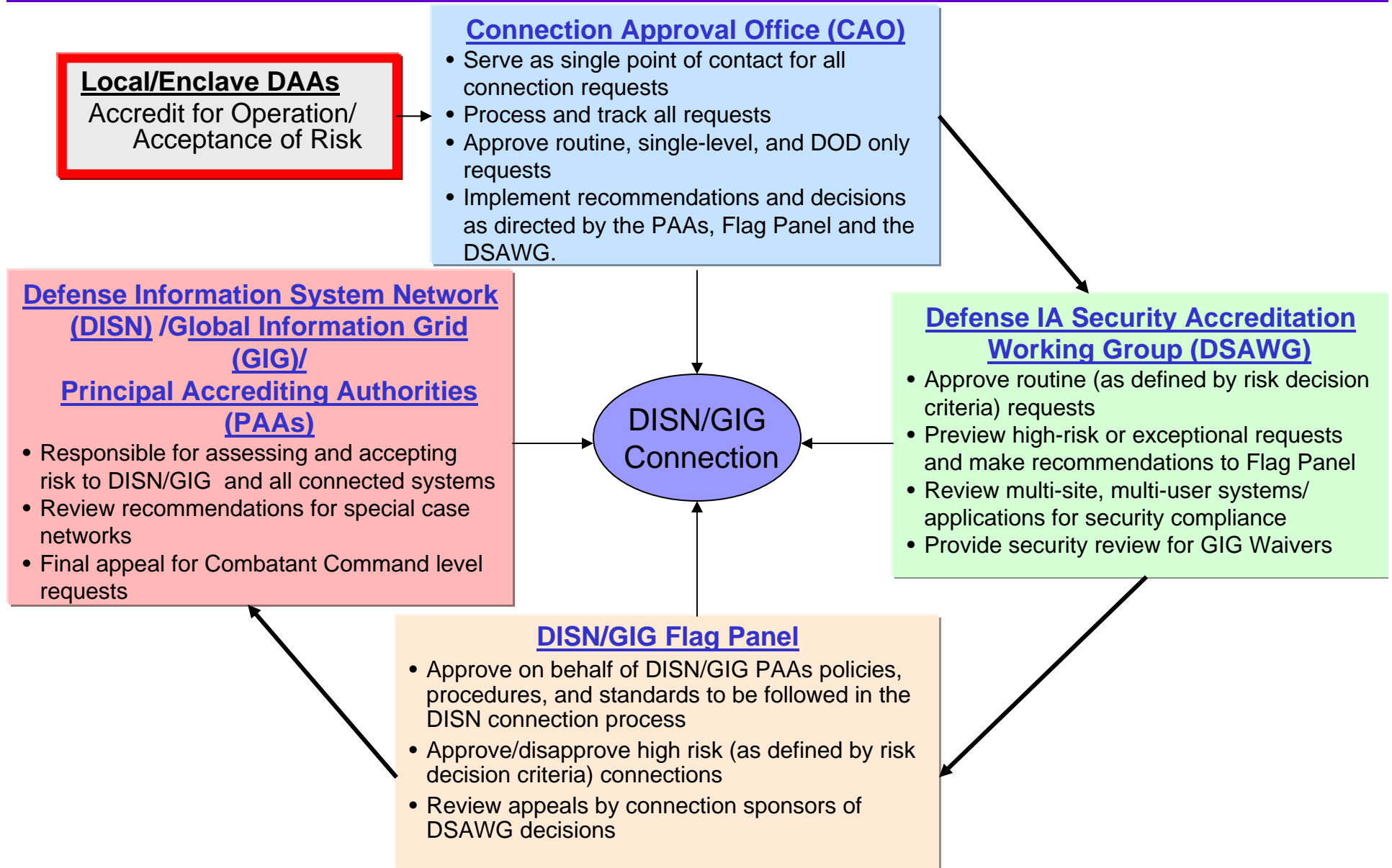
## Responsibilities

- Serve as a community forum for reviewing and resolving authorization and connection decisions related to the sharing of IA and security risks as authorized by DISN/GIG Flag Panel.
- Advise DISN/GIG Flag Panel, the DoD SIAO, and affected DAAs on authorization and connection decisions.
- Assess community-wide risks associated with:
  - DISN/GIG cross-domain interconnections,
  - multiple security level technologies installed on a DISN/GIG-supported infrastructure,
  - and new or unproven technologies and security solutions.
- Assess local and community-wide risks resulting from the use of:
  - commercial infrastructures for DISN/GIG traffic,
  - DISN-interconnected systems accessed by foreign nationals,
  - and the use of known technologies in a DISN/GIG environment for which they have not previously been approved.
- Review certification and accreditation strategies for proposed multi-site, multi-user systems that rely on the DISN/GIG transport.

Unclassified











# The Accreditors





# IA Community Representation

## DISN/GIG Flag Panel Representatives

-  - Chair – (Provided by Joint Chiefs of Staff (JCS/J6))
-  - Undersecretary of Defense-OUSD(I) or Intelligence PAA representative
-  - Undersecretary of Defense-OUSD(AT&L) or BMA PAA representative
-  - DOD Chief Information Office-CIO or EIEMA PAA representative.
-  - Defense Intelligence Agency
-  - National Security Agency
-  - Defense Information Systems Agency
-  - ADNI/CIO – (Advisory Member)

## DSAWG Representatives

- Chair (non voting, provided by DISA)
-  - Defense Intelligence Agency (DIA)
-  - Defense Information Systems Agency (DISA)
-  - Joint Staff (JS)
-  - National Security Agency (NSA)
- Service Representatives:
  - U.S. Air Force
  - U.S. Army
  - U.S. Marine Corps
  - U.S. Navy
-  - Office of the Director of National Intelligence (DNI CIO)
-  - OSD Deputy CIO (DCIO)/Defense-Wide Information Assurance Program (DIAP)
-  - OUSD Deputy for Intelligence – OUSD(I)
-  - OUSD AT&L – (AT&L)
-  - US Strategic Command (USSTRATCOM)
-  - Unified Cross Domain Management Office (UCDMO) (advisory)

Unclassified



# **PPSM – DoD Ports, Protocols, and Services Management**

**Unclassified**



- **PPSM exists to establish a baseline for:**
  - **Security (minimize vulnerabilities) across all network boundaries**
  - **Interoperability across entire network without re-engineering (Net-Centricity)**
  
- **Allow communication through all DoD boundary protection perimeters using the ports, protocols and services approved by the Technical Advisory Group, Configuration Control Board, and the DSAWG.**





# PPSM Policy

---

- **DoDI 8551.1 “*Ports, Protocols, and Services Management*”**
- **Applies to all existing, new and planned DoD Information Systems with Ports, Protocols, and Services (PPS) managed by the DoD Components. All PPS will:**
  - **Utilize the most current PPSM Category Assurance List (CAL) and the Vulnerability Assessment (VA) report**
  - **Implement as described in the most current version of the DISA-issued STIG (Security Technical Implementation Guide).**
  - **Undergo a vulnerability assessment; be assigned an assurance category; be appropriately registered in the PPSM database; and be regulated based on their potential to cause damage to DoD operations and interests**
  - **Be maintained on a central PPSM Registry that will be available to all the DoD Components**
  - **When configured according to the PPSM and the STIGs, be guaranteed the ability to communicate through all DoD boundary protection mechanisms**

**Unclassified**



---

# **CAO – Classified and Unclassified Connection Approval Offices**

**Unclassified**



# Current Connection Approval Environment

---

- **CAOs ensure compliance with Federal, DOD, JS connection policies**
- **Track network security through:**
  - **Cross Domain Solution Tracking**
  - **Systems/Network Approval Process (SNAP) database (Unclass)**
  - **SIPRNet GIAP Security (SGS) database**
- **Currently manage SIPR, NIPR, Voice, Video, VoSiP connection approvals**
  - **All have different connection approval processes**
- **Each DISN Service Manager has own connection guidance**
  - **Different formats, lack of centralized guidance location for customers**
- **Different process/approval chains for DoD/Non-DoD customers**
- **New customers often frustrated by lack of single “Start” point**
  - **“How do I start?” “Who do I talk to?” “Who do you know at DISA?”**

**Unclassified**



# Connection Delay Causes

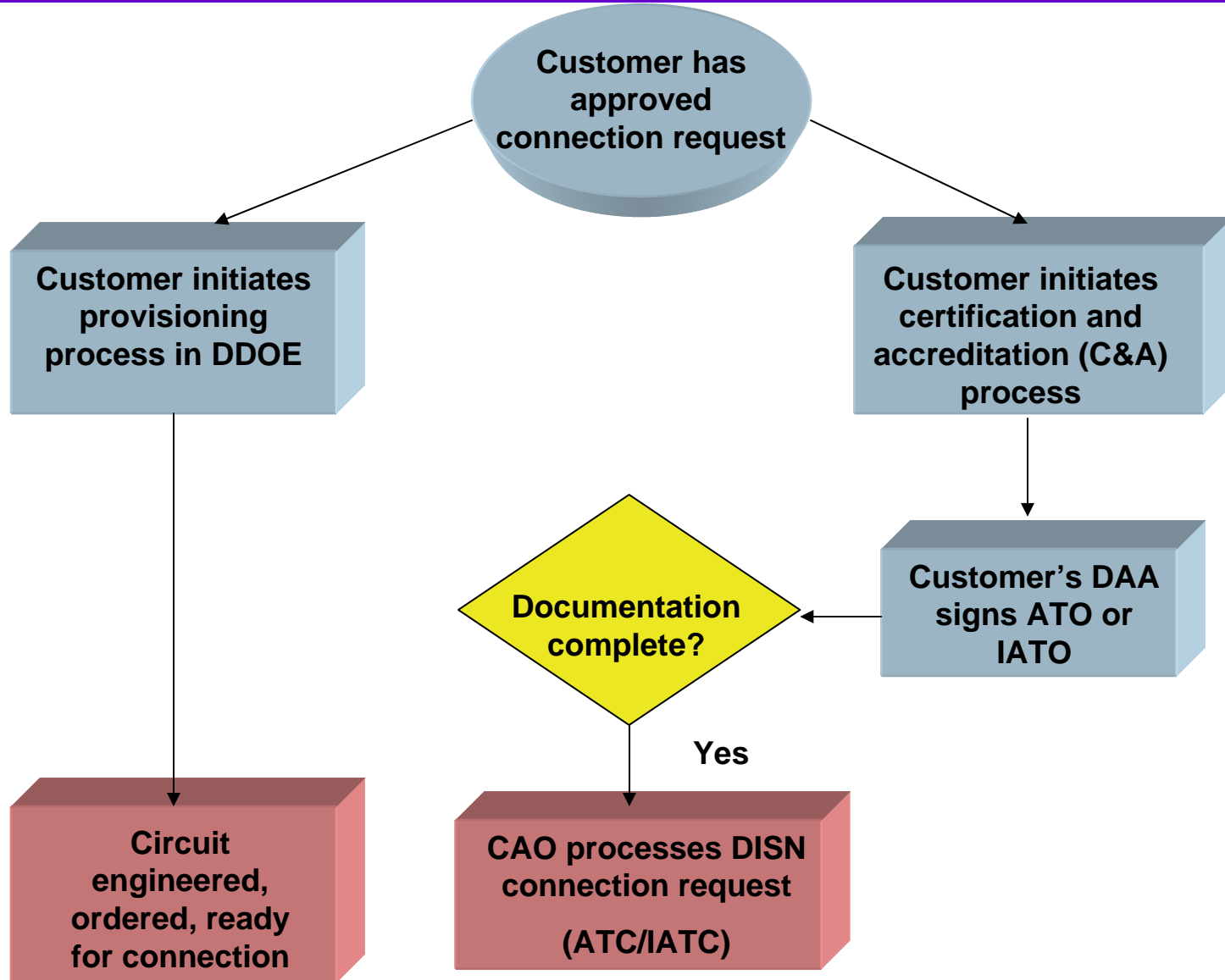
---

- **Classified**
  - Incomplete packages (ATO/IATO, Questionnaire, topology, Consent To Monitor, Statement of Residual Risk, IP registration)
  - Failed scan on new circuit
  - Customer delays resolving remote assessment findings (Retina Scan)
- **Unclassified**
  - Incomplete packages (ATO/IATO, failure to register in SNAP, missing or incomplete enclave topology documentation)
- **Documentation is the primary evidence used by the CAO and DSAWG to assess risk; reflects enclave quality**
- **Connection not ready (equipment, circuit, crypto, etc.)**
- **Customer provisioning and C&A (DITSCAP/DIACAP) efforts executed serially, or C&A not started at all**
- **Lack of DAA or DoD Sponsor involvement in C&A process**

**Unclassified**



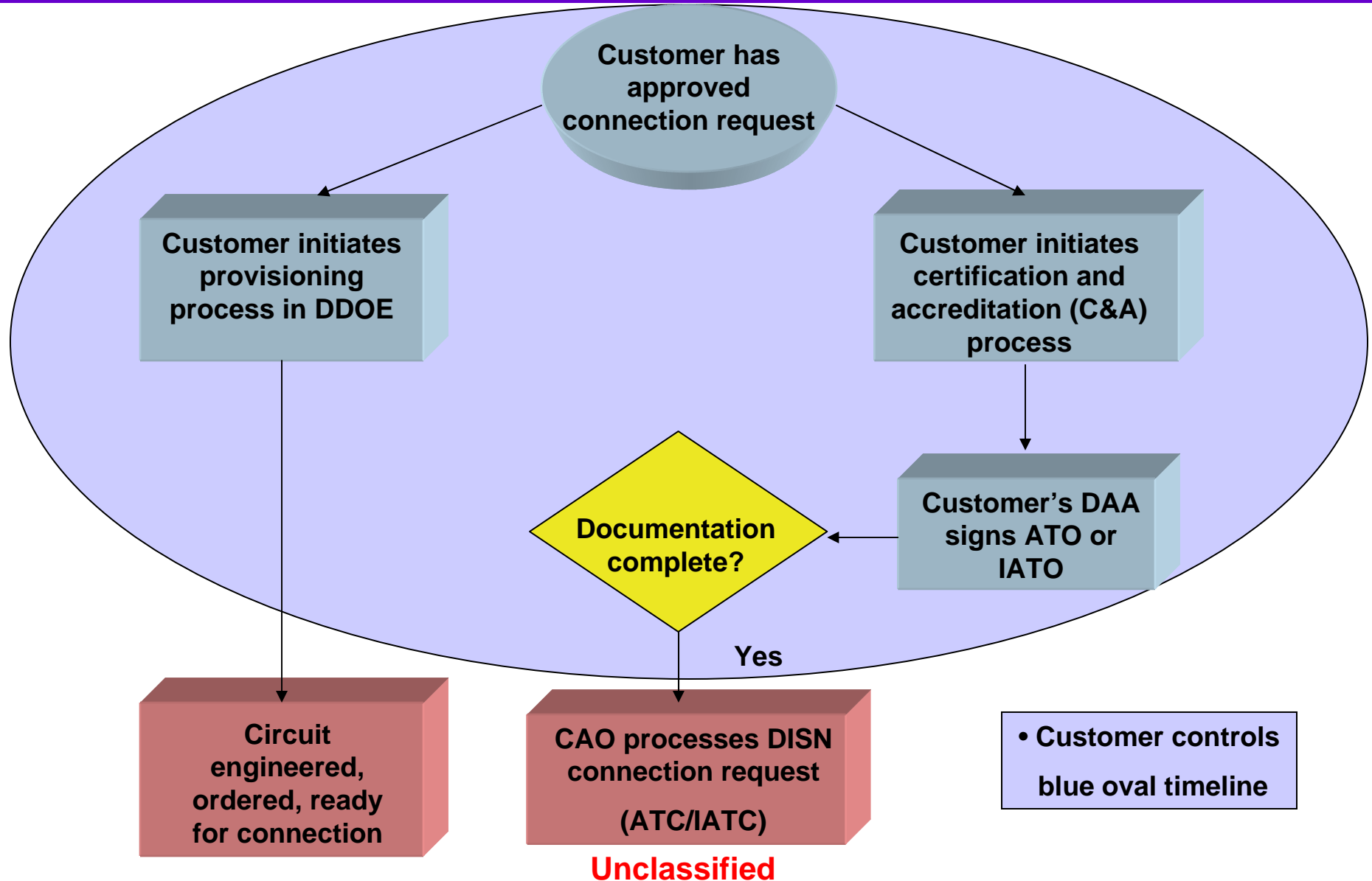
# VERY Simple Connection Process Diagram



**Unclassified**

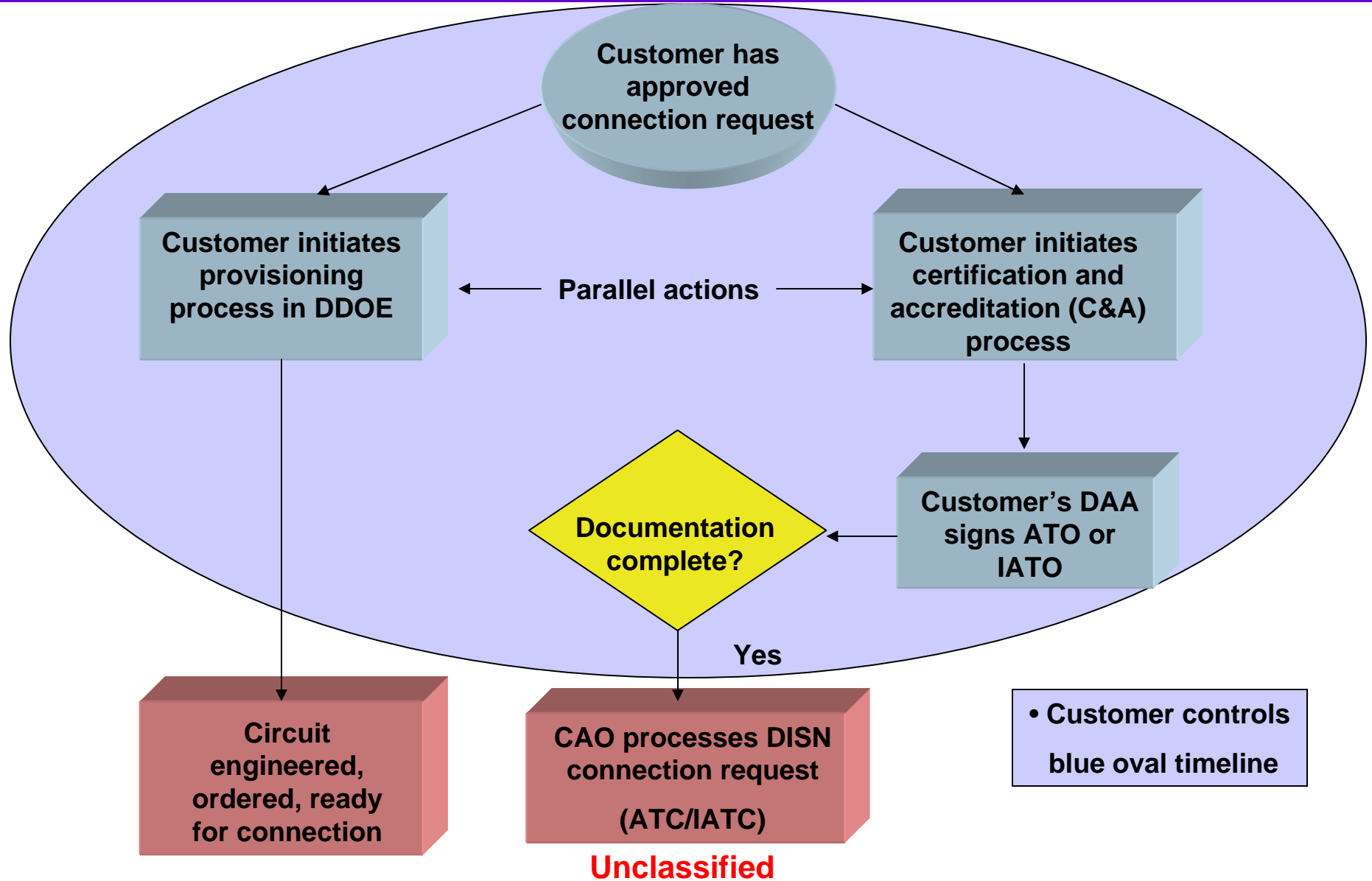


# VERY Simple Connection Process Diagram





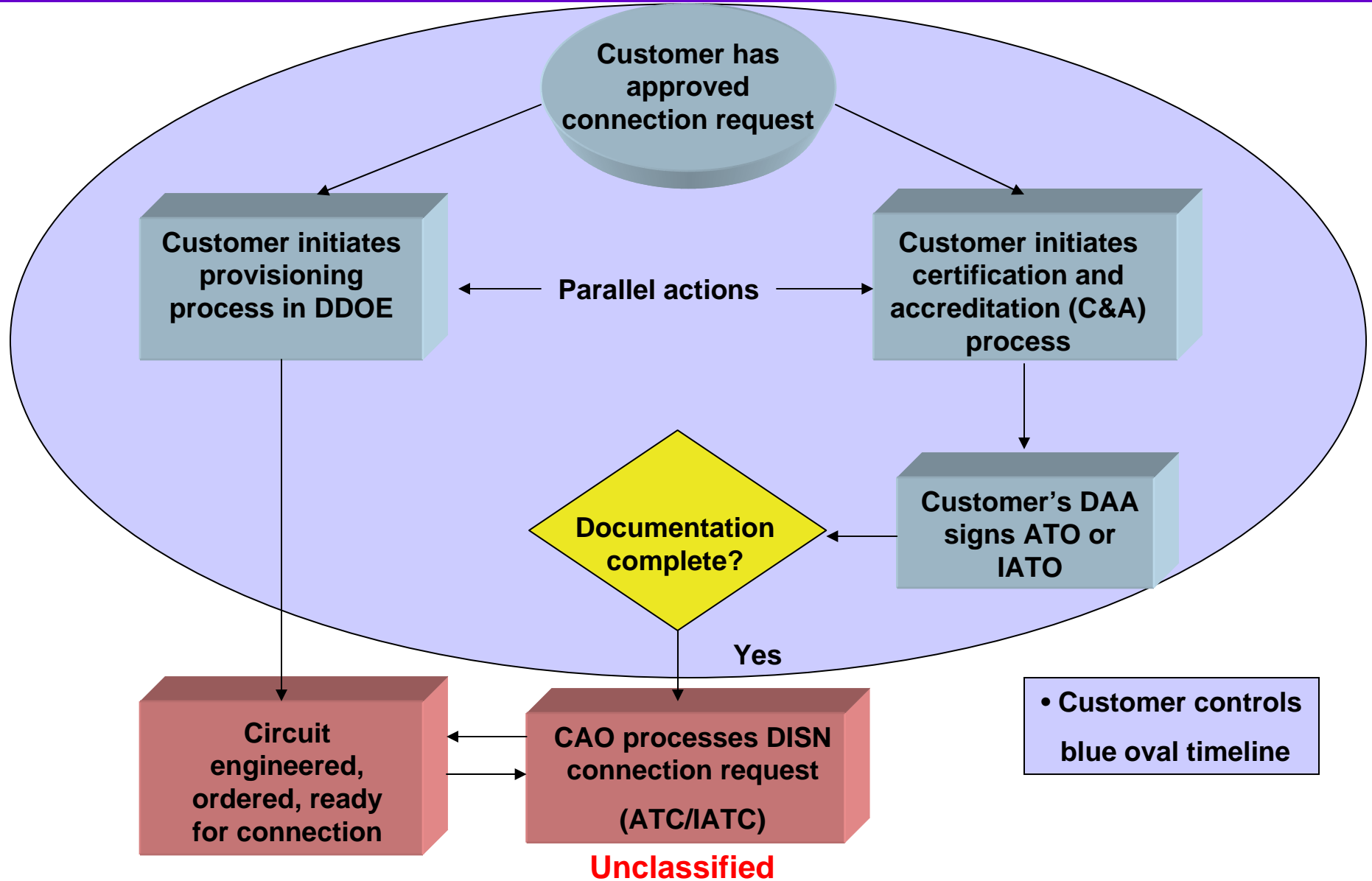
# VERY Simple Connection Process Diagram





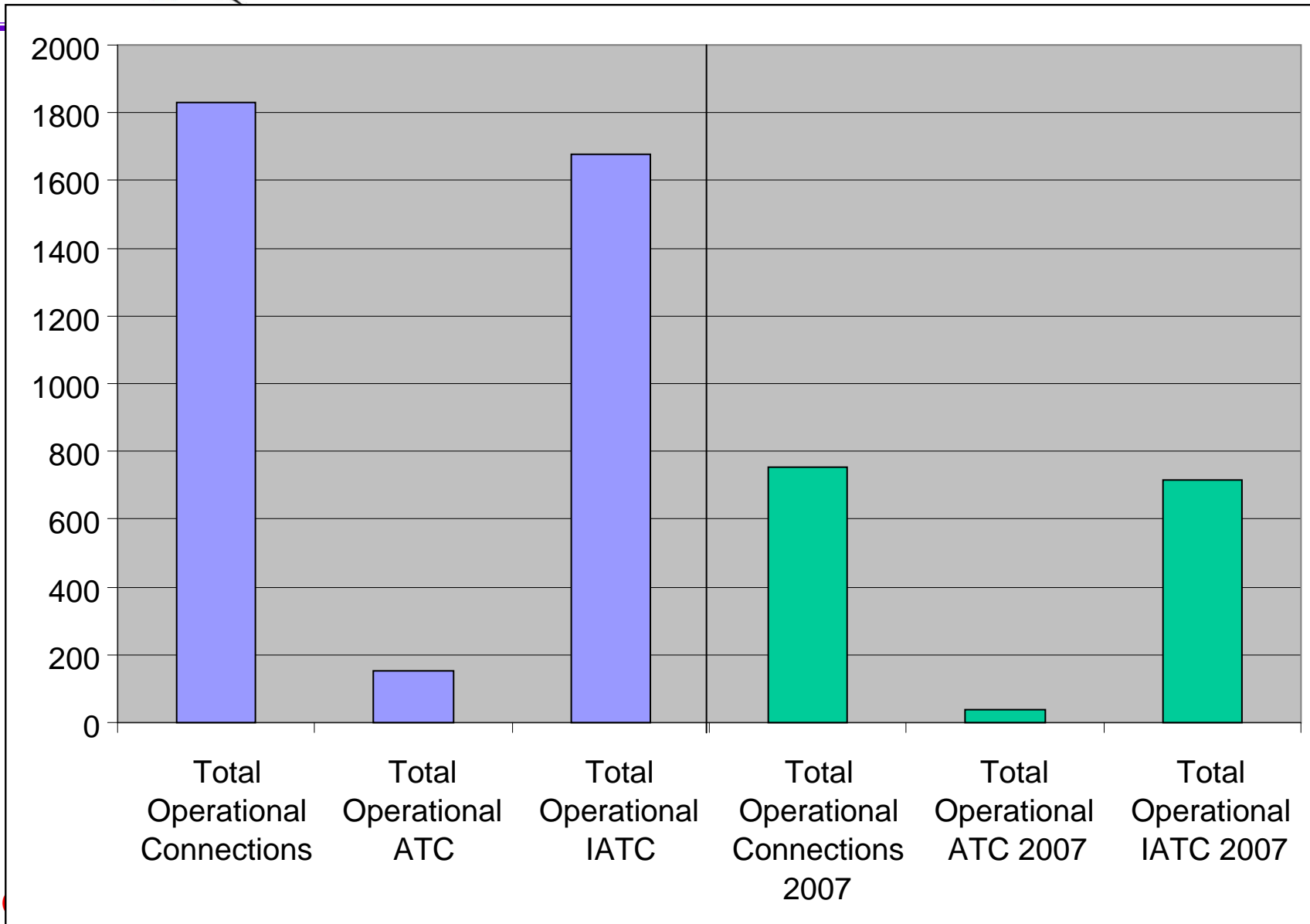


# VERY Simple Connection Process Diagram





# SIPRNet Connection Metrics



is: Unclassified



# Ongoing Improvements

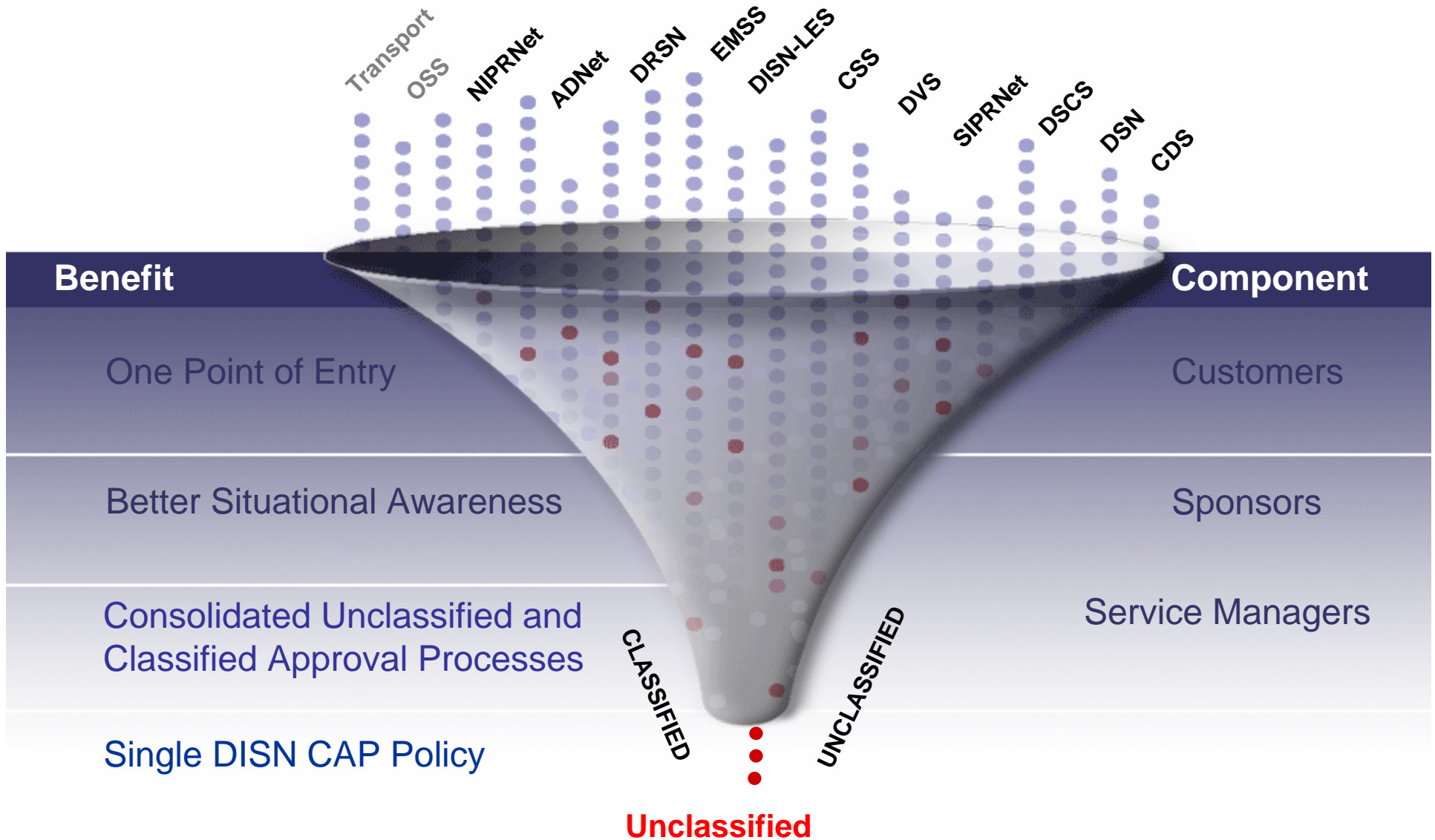
---

- **Focus changed to “Classified” and “Unclassified” connection approval processes vs separate SIPR, NIPR, DSN, VTC, etc.**
  - Eventually add EMSS, Transport, etc.
- **Conducting “Nose-to-Tail” review**
  - Review all internal CAO processes
  - Review all DISN Service Manager (SM) connection processes
  - Scrub/synergize existing connection approval processes
  - Develop single “DISN Connection Process”
  - Identify problems showing up at “Tail” (when ATC/IATC requested)
  - Influence at “Nose”
    - Immediate change: DCCC single POC for new customers
    - Incorporate CAP reqts into ongoing Provisioning Improvement Process
- **Capitalize on on-going IA and information sharing initiatives**
  - DISA Tiger Team, JTF-GNO Cyber Initiative, CIO common DB
- **Develop Web-based DISN Connection Web page**
- **Refine Non-DoD JS validation/OSD approval process**

**Unclassified**



# DISN Connection Approval Goal





# Division Way Ahead

---

- **Establish single connection process for all DISN Services**
  - Consolidate and streamline existing processes to eliminate ambiguities
- **Simplify customer access and process documentation:**
  - **Single DISA entry point for new customers**
    - DCCC (DISN Customer Call Center) (soon)
    - Web site for all connection information, policies, processes
  - **Single DISA exit point**
    - ATC/IATC (Authority to Connect/Interim Authority to Connect)
- **Implement changes, educate customers**
- **Provide improved access to connection information**
  - Seamless access to the SNAP, SGS and PPSM data

Unclassified



# Points of Contact

---

- **Teri C. Netter - 703-882-0326**
  - Chief, DISN Connection Approval Division
- **Dennis Ruth – 703-882-0096**
  - DSAWG Chair
- **James Conway – 703-882-2144**
  - Classified Connection Approval Office
- **Priscilla Patterson – 703 -882-0133**
  - Unclassified Connection Approval Office
- **Curtis J. Davis – 703-882-0296**
  - Ports, Protocols, and Services Management Office

**(For all contacts: DSN 381-xxxx)**

**Unclassified**



---

**Questions?**

**Unclassified**



# Backup

Unclassified





# Authority to Connect (ATC) Documentation Requirements

---

1. **Statement of Accreditation (Interim Approval to Operate [IATO] or Approval to Operate [ATO]) signed by Designated Approving Authority (DAA)**
  - Approval to Operate (ATO) - Valid for up to three years
  - Interim Approval to Operate (IATO) signed by DAA -Valid for up to six months.
    - Statement of Residual/Significant Risk, Mode of Operations, and Maximum level of sensitivity/classification of information being processed must be included.
2. **Enclave Topology Diagram - Most recent configuration to include firewall(s), IDS, PC's, user terminals, servers, hubs, bridges, routers, major applications (i.e. –GCCS, CIS, DMS), gateways, modems, card readers, backup devices, room and building number, and switches (mechanical –A/B or electrical), backside connections, IP addresses, encryption devices and CrossDomain Solutions (formerly Secret and Below Interoperability (SABI) - High Assurance Guards (HAG)/ boundary crossing/interface devices). Topology must be dated and signed by IAM/IAO.**
3. **Consent to Monitor signed by the DAA.**
4. **If SIPRNet, a SIPRNET Connection Questionnaire (SCQ), dated 01 October 2006**
5. **If NIPRNet, user must complete SNAP registration**
6. **Site system security documentation including specific security features and implementations IAW DODD 8500.1 and the DIACAP, must be available upon request**
7. **Successful completion of a remote compliance assessment by the DISA SCAO Team**
8. **SIPRNet IP Registration –All IP's must be registered -Contact the SIPRNet Support Center at 800-365-3542) The use of private IP address space (non-routable IPs) is not permitted on the SIPRNet. Reference NIC Registry Protocol 9802, 30 Oct 2002, <http://www.nic.mil/ftp/mgt/ptl-9802.txt>**

**Unclassified**



[www.disa.mil](http://www.disa.mil)

---

---