DEFENSE INFORMATION SYSTEMS AGENCY

DSN CONNECTION GUIDE

VERSION May 23, 2005

DRAFT

TABLE OF CONTENTS

1 INTRODUCTION

In the past, DSN voice equipment was purchased according to the needs and the selection of the individual Services. Security was enforced by the individual Services at a local level.

While data systems have always been required to perform security testing on their systems, the voice world has not. However, in a world of terrorists, hackers and high-level technology, the DSN faces greater risks than it did in simpler times. For this reason, policy DoDI 8100.3, *DoD Voice Networks*, 16 January 2004, requires DoD voice networks to be interoperable and security certified and accredited.

Each of us impacts the safety of our country's assets which could be compromised by a security breach. In the case of the DSN, we are not protecting just hardware and software, we are protecting peoples' lives, and supporting counterterrorism and the prevention of war. You need to understand that securing the DSN is not just a lot of unnecessary paperwork. The threats are very real, and we need to establish a low-risk DSN, with the key focus being on the DSN voice equipment.

1.1 PURPOSE

This *Connection Guidance* document was developed to provide helpful and detailed guidance to the DoD components for certification and accreditation of voice equipment connected to the DSN. The sections are structured to provide the reader with a 'how-to' approach to these processes. The purpose of this guide is to allow sites to evaluate their DSN voice equipment to determine if they have an Authority To Operate (ATO) 'Low Risk' or not 'High Risk', and to follow the enclosed procedures for each. This document discusses how certification and accreditation testing is done, identifies procedures that DoD components can use to come into compliance with interoperability and information assurance requirements, and defines the risk analysis process for your DSN voice equipment.

TIP

You do not need to read this entire document, only the sections that address the status of your DSN voice equipment.

1.2 AUDIENCE

This document is directed to the personnel of each DoD base/post/camp/station. It is an informal, information guidance document meant to direct and enable people at the site level to properly protect their DSN voice equipment.

2 OVERVIEW

There are three basic requirements for DSN voice equipment: (1) DSN voice equipment that is purchased must be on the Approved Products List, (2) it must be site-accredited via an ATO, and (3) it must receive Authority to Connect (ATC) from the DSN Single System Manager (SSM).

There are a number of different elements involved in each of the individual processes associated with these three requirements. The following three are the main DISA elements involved that anyone attempting to fulfill the requirements for connection to the DSN will need to be familiar with.

Voice Connection Approval Office (VCAO)

The VCAO is the starting point for any of the three basic requirements for DSN voice equipment because it is the focal point for the following DSN management activities.

- JITC interoperability (IO) and information assurance (IA) test requests, requirements, scheduling, and Approved Products List (APL) management for the DSN.
- DSN ATC request processing, approval, and notification.
- Local site Defense Information Technology Security Certification and Accreditation Process (DITSCAP) assistance and monitoring agent for the DSN.

The VCAO manages both the APL maintained on the JITC homepage, as well as the JITC test submittal request form maintained on the DSN homepage. The VCAO is also responsible for development and maintenance of the Authority to Connect request form, which is also maintained on the DSN homepage.

A small section of the VCAO specializes in DITSCAP as well and is responsible for providing assistance and monitoring the completion status of the local DITSCAP for all bases, camps, posts, and stations that have DSN voice equipment. The VCAO is a good starting point for guidance on completing the local DITSCAP for DSN voice equipment. (Please refer to Appendix B for further information about the VCAO.)

Joint Interoperability Certification (JIC) Test Team

The JIC Test Team consists of members of the engineering staff located at JITC, Ft. Huachuca, Arizona. Once the JIC Action Officer (AO) receives a VCAO Test Submittal Form with a VCAO Tracking Number assigned, the proposed solution(s) are analyzed against the DoD Voice Networks Generic Switching Center Requirements (GSCR) for technical requirements. The JIC AO is responsible for contacting the DoD sponsor of the proposed test for implementation requirements, and maintaining contact with the sponsor throughout the testing process for updates and changes. The JIC AO is also responsible for contacting the vendor for technical documentation, Letters of Compliance, and to discuss funding requirements. The JITC AO is the POC for coordination with the vendor for all equipment delivery and setup at the Joint

Interoperability Test Command, Ft. Huachuca, AZ. (Please refer to Appendix B for further information about the JIC Test Team.)

Information Assurance Test Team (IATT)

The Information Assurance Test Team consists of members of the DISA Global Information Grid (GIG) Enterprise Services (GES) engineering staff and Air Force Information Warfare Center (AFIWC). The majority of all Information Assurance testing is conducted at the JITC, Ft. Huachuca, Arizona. An additional smaller portion is conducted in San Antonio, Texas at AFIWC. Once the IATT AO receives a VCAO Test Submittal Form with a VCAO Tracking Number assigned, the proposed solution(s) are analyzed against the Information Assurance Test Plan (IATP) for technical requirements. The IATT AO is responsible for contacting the DoD sponsor of the proposed test for implementation requirements, and maintaining contact with the sponsor throughout the testing process for updates and changes. The IATT AO is also responsible for contacting both the vendor and sponsor for technical documentation. The IATT will contact both the vendor and sponsor of a solution to coordinate an Inbrief to discuss in the IA process, the solution, the testing scope, and test scheduling in detail prior to testing a solution. Upon completion of testing the IATT will coordinate with the vendor and sponsor of a product to hold an Outbrief to discuss in detail the results of the IA testing. (Please refer to Appendix B for further information about the JIC Test Team.)

3 DSN VOICE EQUIPMENT REQUIREMENTS

There are three basic requirements for DSN voice equipment: (1) DSN voice equipment must be purchased from the APL, (2) it must be site-accredited via an ATO, and (3) it must receive ATC from the DSN SSM. While all existing DSN voice equipment will be upgraded or replaced over a period of time, it is mandatory that a DITSCAP be performed on existing DSN voice equipment at DSN locations. Site accreditation consists of a completed System Security Authorization Agreement (SSAA) and an ATO letter signed by the Designated Approving Authority (DAA).

3.1 DSN VOICE EQUIPMENT COMPLIANCE LEVEL CATEGORIES

In this document, DSN voice equipment is categorized into four main groups based on their compliance levels. Two of these compliance levels result in conditions of 'High-Risk' conditions for DSN voice equipment. The other two compliance levels result in either 'Medium-Risk' or 'Low-Risk' conditions for DSN voice equipment.

Category	Description	Is Equipment Listed on APL Website	Site level ATO	Risk level
A	NO APL & NO ATO	NO	NO	HIGH
B	APL & NO ATO	YES	NO	HIGH
C	NO APL, WITH ATO	NO	YES	MEDIUM
D	APL & ATO	YES	YES	LOW

The following definitions and explanations are items listed in this document, and elaborate on the items in the matrix above. Most of the existing DSN voice equipment will fall within either Category A or B below.

<u>Category A</u>: NO APL & NO ATO – In this category, DSN voice equipment neither appears on the DSN Approved Products List (APL) nor has received a formal ATO document (i.e., a signed DAA letter). The main focus of this section will be to show the owners of DSN voice equipment that are not on the APL what to do. This category is considered to be 'High-Risk'.

<u>Category B</u>: APL & NO ATO – It is important that the site properly accredits all DSN voice equipment. In this category, DSN voice equipment is included in the APL, but has not received a site accreditation or an ATO. Until the DSN voice equipment has an ATO, it is still considered to be 'High-Risk'.

Category C: **NO APL, WITH ATO –** As mentioned above, most DSN voice equipment was purchased prior to the creation of the APL website. In this case, your DSN voice equipment does not appear on the APL, but you have a site ATO for DSN. In this situation, your DSN voice equipment is considered to be 'Medium-Risk'.

Category D: **APL & ATO –** DSN voice equipment in this category is relatively new equipment. It has been properly accredited by the local DAA for an ATO. Review our section in this document to confirm that nothing was missed during the accreditation process, and that you have applied for an ATC from the VCAO.

3.2 WHAT TO DO

3.2.1 DSN Voice Equipment Compliance Evaluation

Evaluate your DSN voice equipment and determine which category from the previous section best describes the risk level of your equipment, thereby identifying the actions you need to take to bring your DSN voice equipment to the 'Low Risk' level.

3.2.2 Check the APL Website

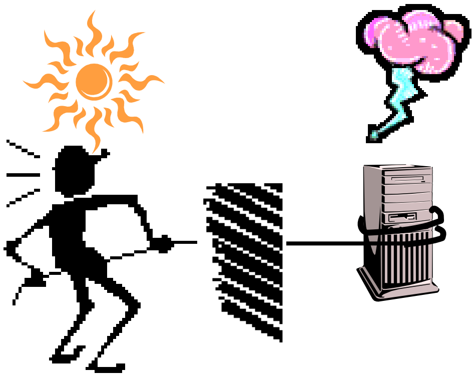
Check the APL on the web located at **http://jitc.fhu.disa.mil/tssi/apl.html**. It is a requirement of DoDI 8100.3 that new DSN voice equipment must be purchased from the APL. All items on the APL are required to have been certified and accredited for IO and IA.

TIP

If you do not have a signed approval letter from your site DAA (i.e., no ATO) the DSN voice equipment is considered 'High Risk'.

4 ACTIONS FOR CATEGORY A (NO APL & NO ATO)

Although Category A configurations are considered to be 'High Risk', it may be possible to make your DSN voice equipment 'Low Risk' by performing the actions listed in section 4.1.



4.1 CATEGORY A STEPS FOR COMPLIANCE

Category A includes those systems that are NOT on the APL list, and have not received an ATO. For systems in this category, all of the steps listed below in sections 4.1.1, 4.1.2, and 4.1.3 shall be completed.

4.1.1 APL Product Submission – JIC and IA Testing

- **Verify that the product is not already on the APL (see http://jitc.fhu.disa.mil/tssi/apl.html), or is not already scheduled for testing at JITC (see http://jitc.fhu.disa.mil/tssi/schedule.html).**
- **Identify a Government sponsor for the product. (See Sponsorship topic in Appendix B, under the VCAO section.)**
- **Prepare a topology diagram of the system to be tested.**
- **Access http://www.disa.mil/gs/dsn/jic/index.html to fill out the on-line submittal form.**
- **The VCAO will contact you regarding the test dates and the outcome of the testing.**

4.1.2 Local DITSCAP ATO Procedures

- **Once the product is on the APL list as IO certified and IA accredited, follow the next steps for authority to connect.**
- **Have your ISSO/IAO perform a compliance validation using the appropriate STIGs and STIG checklists. A copy may be obtained from the Field Security Office (FSO) Help Desk at mailto:fso_spt@ritchie.disa.mil.**

- **Have your ISSO/IAO confirm that the hardware/software has the same configuration as indicated in the interoperability certification letter. A copy may be obtained from http://jitc.fhu.disa.mil/tssi/apl.html.**
- **Have your ISSO/IAO read the DSN voice equipment IA test reports to ensure that all vulnerabilities have been mitigated per installation. A copy may be obtained by email from the VCAO at NS534-web@ncr.disa.mil.**
- **Ensure that your local SSAA has been updated to include all aspects of your specific DSN configuration.**
- **Ensure that an Authority to Operate memo has been written, and signed by the local DAA, for the specific DSN configuration.**

4.1.3 Authority to Connect

- **Request an ATC from the DSN SSM by completing the On-Line ATC submittal form at http://www.disa.mil/gs/dsn/jic/atcsubmittal.html.)**
- **The VCAO will validate the submission, and request additional information, if required.**
- **Once the request has been successfully validated, the DSN SSM will issue an interim authority to connect (IATC)/ATC dependent on the certification and accreditation status of the DSN voice equipment. (Note: An ATC is good for 3 years, while an IATC timeframe may vary. A copy of the IATC/ATC memo, signed by the local DAA for the DSN voice equipment, is required for an IATC/ATC.)**

The DSN VCAO may be contacted at email: NS534-web@ncr.disa.mil.

4.2 TEMPLATE FOR SSAA

A DITSCAP SSAA template has been created for unclassified voice networks and is available on the DSN website (http://www.disa.mil/gs/dsn/index.html). Note that the Appendices must also be attached with the proper information and that a DAA letter is an attachment to the SSAA. The IASE site (located at http://iase.disa.mil/ditscap) provides additional information regarding DITSCAP.

TIP

Some DoD Components have an SSAA for each base/post/camp/station, while others have an SSAA for each command. The acquiring activity is required to submit an Accreditation Letter from the Component DAA to the VCAO in order to be approved for an ATC. The Accreditation Letter, generally an attachment to the SSAA, is a statement from the DAA that the system is operating at an acceptable level of risk. (see DoDI 5200.40: http://www.dtic.mil/whs/directives/corres/html/520040.htm)

5 ACTIONS FOR CATEGORY B (APL & NO ATO)

Although Category B configurations are considered to be 'High Risk', it may be possible to make your DSN voice equipment 'Low Risk' by performing the actions listed in section 5.1.

5.1 CATEGORY B STEPS FOR COMPLIANCE

Category B includes those systems that are on the APL list, and have not received an ATO. Even if the product is on the APL, you must perform the following tasks in bold print for ATO and ATC before you can install it. (If the product is on the APL, the steps in section 5.1.1, in non-bold type may be omitted for solutions in this category.)

5.1.1 APL Product Submission – JIC and IA Testing

- Verify that the product is not already on the APL (see http://jitc.fhu.disa.mil/tssi/apl.html), or is not already scheduled for testing at JITC (see http://jitc.fhu.disa.mil/tssi/schedule.html).
- Identify a Government sponsor for the product. (See Sponsorship topic in Appendix B, under the VCAO section.)
- Prepare a topology diagram of the system to be tested.
- Access www.disa.mil/gs/dsn/jic/index.html to fill out the online submittal form.
- The VCAO will contact you regarding the test dates and the outcome of the testing.

5.1.2 Local DITSCAP ATO Procedures

- ❖ **Once the product is on the APL list as IO certified and IA accredited, follow the next steps for authority to connect.**
- ❖ **Have your ISSO/IAO perform a compliance validation using the appropriate STIGs and STIG checklists. A copy may be obtained from the FSO Help Desk at mailto:fso_spt@ritchie.disa.mil.**
- ❖ **Have your ISSO/IAO confirm that the hardware/software has the same configuration as indicated in the interoperability certification letter. A copy may be obtained from http://jitc.fhu.disa.mil/tssi/apl.html.**
- ❖ **Have your ISSO/IAO read the DSN voice equipment IA test reports to ensure that all vulnerabilities have been mitigated per installation. A copy may be obtained by email from the VCAO at mailto:NS534-web@ncr.disa.mil.**

- **Ensure that your local SSAA has been updated to include all aspects of your specific DSN configuration.**
- **Ensure that an Authority to Operate memo has been written, and signed by the local DAA, for the specific DSN configuration.**

5.1.3 Authority to Connect Steps

- **Request an ATC from the DSN SSM by completing the Online ATC submittal form at http://www.disa.mil/gs/dsn/jic/atcsubmittal.html.)**
- **The VCAO will validate the submission, and request additional information, if required.**
- **Once the request has been successfully validated, the DSN SSM will issue an IATC/ATC dependent on the certification and accreditation status of the DSN voice equipment. (Note: An ATC is good for 3 years, while an IATC timeframe may vary. A copy of the IATC/ATC memo, signed by the local DAA for the DSN voice equipment, is required for an IATC/ATC.)**

The DSN VCAO may be contacted at email: NS534-web@ncr.disa.mil.

TIP

An IATC is issued to sites that have requested to connect to the DSN, but have not met all of the necessary requirements for receiving an ATC. The length of time for which an IATC is issued is based on the local DITSCAP status of the site requesting connection of their voice equipment to the DSN. If the voice equipment being submitted for connection is not on the APL and does not have an ICTO, an IATC will not be granted.

6 ACTIONS FOR CATEGORY C (NO APL, WITH ATO)

6.1 CATEGORY C STEPS FOR COMPLIANCE

Category C includes those systems that are NOT on the APL list, but have received an ATO. For systems in this category, all of the steps listed below in this section in bold print shall be completed. (The steps in section 6.1.2, indicated with the '•' symbol in non-bold type, may be omitted for solutions in this category.)

6.1.1 APL Product Submission – JIC and IA Testing

- ❖ **Verify that the product is not already on the APL (see http://jitc.fhu.disa.mil/tssi/apl.html), or is not already scheduled for testing at JITC (see http://jitc.fhu.disa.mil/tssi/schedule.html).**
- ❖ **Identify a Government sponsor for the product. (See the Sponsorship topic in Appendix B, under the VCAO section.)**
- ❖ **Prepare a topology diagram of the system to be tested.**
- ❖ **Access http://www.disa.mil/gs/dsn/jic/index.html to fill out the on-line submittal form.**
- ❖ **The VCAO will contact you regarding the test dates and the outcome of the testing.**

6.1.2 Local DITSCAP Steps for ATO

- Once the product is on the APL list as IO certified and IA accredited, follow the next steps for authority to connect.
- Have your ISSO/IAO perform a compliance validation using the appropriate STIGs and STIG checklists. A copy may be obtained from the Field Security Office (FSO) Help Desk at mailto:fso_spt@ritchie.disa.mil.
- Have your ISSO/IAO confirm that the hardware/software has the same configuration as indicated in the interoperability certification letter. A copy may be obtained from http://jitc.fhu.disa.mil/tssi/apl.html.
- Have your ISSO/IAO read the DSN voice equipment IA test reports to ensure that all vulnerabilities have been mitigated per installation. A copy may be obtained by email from the VCAO at mailto:NS534-web@ncr.disa.mil.
- Ensure that your local SSAA has been updated to include all aspects of your specific DSN configuration.
- Ensure that an Authority to Operate memo has been written, and signed by the local DAA, for the specific DSN configuration.

6.1.3 Authority to Connect Steps

- **Request an ATC from the DSN SSM by completing the On-Line ATC submittal form at http://www.disa.mil/gs/dsn/jic/atcsubmittal.html.)**
- **The VCAO will validate the submission, and request additional information, if required.**
- **Once the request has been successfully validated, the DSN SSM will issue an IATC/ATC dependent on the certification and accreditation status of the DSN voice equipment. (Note: An ATC is good for 3 years, while an IATC timeframe may vary. A copy of the IATC/ATC memo, signed by the local DAA for the DSN voice equipment, is required for an IATC/ATC.)**

The DSN VCAO may be contacted at email: NS534-web@ncr.disa.mil.

TIP

If the solution being requested for ATC is a PBX-2, owned by a component of the DoD, then a waiver from the Joint Staff to the requirement for Military Unique Features (MUF), mandated by CJCSI 6215.01B must be requested and approved prior to the site receiving an IATC/ATC. Contact the VCAO for further information regarding the requirement for MUF.

7 ACTIONS FOR CATEGORY D (APL AND ATO)

Category D includes DSN voice equipment that is listed on the APL, AND has received an ATO. They are considered to be ‘Low Risk’ because they:

- Were purchased from the APL
- Have been JIC and IA accredited
- Have had DITSCAP performed on them
- Have been validated via STIGs

7.1 CATEGORY D STEPS FOR COMPLIANCE

Category D includes those systems that are on the APL list, and have received an ATO. For systems in this category, only the steps listed below in section 6.1.3 in bold print must be completed in order to obtain an ATC. (The steps in sections 7.1.1 and 7.1.2, indicated with the ‘•’ symbol and in non-bold type, may be omitted for solutions in this category.)

7.1.1 APL Product Submission – JIC and IA Testing

- Verify that the product is not already on the APL (see http://jitc.fhu.disa.mil/tssi/apl.html), or is not already scheduled for testing at JITC (see http://jitc.fhu.disa.mil/tssi/schedule.html).
- Identify a Government sponsor for the product. (See the Sponsorship topic in Appendix B, under the VCAO section.)
- Prepare a topology diagram of the system to be tested.
- Access www.disa.mil/gs/dsn/jic/index.html to fill out the on-line submittal form.
- The VCAO will contact you regarding the test dates and the outcome of the testing.

7.1.2 Local DITSCAP ATO Procedures

- Once the product is on the APL list as IO certified and IA accredited, follow the next steps for authority to connect.

- Have your ISSO/IAO perform a compliance validation using the appropriate STIGs and STIG checklists. A copy may be obtained from the Field Security Office (FSO) Help Desk at mailto:fso_spt@ritchie.disa.mil.
- Have your ISSO/IAO confirm that the hardware/software has the same configuration as indicated in the interoperability certification letter. A copy may be obtained from http://jitc.fhu.disa.mil/tssi/apl.html.
- Have your ISSO/IAO read the DSN voice equipment IA test reports to ensure that all vulnerabilities have been mitigated per installation. A copy may be obtained by email from the VCAO at mailto:NS534-web@ncr.disa.mil.
- Ensure that your local SSAA has been updated to include all aspects of your specific DSN configuration.
- Ensure that an Authority to Operate memo has been written, and signed by the local DAA, for the specific DSN configuration.

7.1.3 Authority to Connect Steps

- **Request an ATC from the DSN SSM by completing the On-Line ATC submittal form at http://www.disa.mil/gs/dsn/jic/atcsubmittal.html.)**
- **The VCAO will validate the submission, and request additional information, if required.**
- **Once the request has been successfully validated, the DSN SSM will issue an IATC/ATC dependent on the certification and accreditation status of the DSN voice equipment. (Note: An ATC is good for 3 years, while an IATC timeframe may vary. A copy of the IATC/ATC memo, signed by the local DAA for the DSN voice equipment, is required for an IATC/ATC.)**

The DSN VCAO may be contacted at email: NS534-web@ncr.disa.mil.

TIP

The DoD component is required to update their existing SSAA to accurately reflect DSN hardware/software/firmware at their sites. (If there is no existing SSAA, the DoD component is required to create an SSAA in conjunction with the DITSCAP process.) Open the following link for further information: www.disa.mil/gs/dsn/ia.html.

APPENDIX A: DEFINITIONS AND ACRONYMS

AFIWC (Air Force Information Warfare Center).

AO (Action Officer).

APL (Approved Product List).

ATC (Authority To Connect).

ATO (Authority To Operate).

CA (Certification Authority). The CA is the official who is responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish how well a particular design and implementation meet specified security requirements. There is a DISN CA, responsible for all DISN services, to include the DSN network. Each DoD component base/post/camp/station, or equivalent, also has a CA who is responsible for networks on their installation.

CRADA (Cooperative Research and Development Agreement).

DAA (Local Designated Approving Authority). The DAA is an official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. In the case of DISN, the authority is assigned to four individuals who are members of DISA, DIA, NSA, and the Joint Staff. Each DoD component base/post/camp/station, or equivalent, also has a DAA. The DAA may be delegated in writing by a responsible senior authority. Usually, a DAA is a senior commissioned officer or senior government civilian (i.e., GS-15 or above). DAAs must be both U.S. citizens and DoD employees. DAAs may not also serve as CAs for systems they accredit.

DITSCAP (Defense Information Technology Security Certification and Accreditation Process. The DITSCAP fundamentally establishes a standard procedure for security with regard to the DSN. Each base/post/camp/station is required to have a DAA, a CA, and an SSAA for their IT assets, which includes voice, video, and data. (Additionally, DISA is required to have a DAA [DISN currently has 4 DAAs], a CA, and a SSAA for the DSN Network.) The DoDI 5200.40 provides the procedures for DITSCAP that base/post/camp/station are required to follow. A site SSAA template exists and can be obtained via the DSN web site. DSN DITSCAP is moving toward an automated process shown in Appendix C.

DSAWG (DISN Security Accreditation Working Group). The DSAWG, as requested, performs analysis on all GIG waiver and appeal requests to determine compliance with all appropriate DISN security policies. The DAWG develops recommendations on the acceptability of the waiver/appeal in meeting DISN security policy and whether any DISN security policy waiver should be granted. The DSAWG provides recommendations to DISA as a part of the assessment of the waiver/appeal and to the GIG Waiver Panel Chair."[1] The DSAWG acts as IA expert staff. The DAWG provides input and recommendations to the DISN DAA flag panel.

FID (Facility Identifier).

FSO (Field Security Office).

GES (GIG Enterprise Services).

GIG (Global Information Grid).

GSCR (Generic Switching Center Requirements). DSN GSCR shall specify technical requirements for a telecommunications switch and shall be used to support lease or procurement, and testing of DSN telecommunications switches. The GSCR shall identify the minimum switch requirements and features applicable to the overall DoD community for respective networks. The GSCR shall also define and document interoperability requirements among telecommunications switches that are part of the DSN. The Chairman of the Joint Chiefs of Staff shall validate and ASD (NII)/DoD CIO shall approve DSN GSCR. The DSN Generic Switch Test Plan (GSTP) shall be based on the requirements of the GSCR.

GSTP (Generic Switching Test Plan). DSN GSTP shall specify interoperability test criteria for DSN telecommunications switches connected or planned for connection to the DSN. The GSTP/SSTP shall address interoperability requirements between new technologies and the existing network, as well as the performance impact of these new technologies on MUF.

IA (Information Assurance).

IA C&A (Information Assurance C&A Process). The standard DoD approach for identifying information security requirements, providing security solutions, and managing security of DoD information systems.

IAO (Information Assurance Officer).

IASE (Information Assurance System Environment).

IATC (Interim Authority To Connect).

IATP (Information Assurance Test Plan). The IATP shall provide security features test criteria for voice telecommunications equipment connected or planned-for connection to the DSN. The IATP shall evaluate security features within the existing network and critical areas involving MUF and new telecommunications technology. The IATP shall also address security features between new technologies and the existing network, and the performance impact of these new technologies on MUFs. The IA testing shall be conducted, in accordance with STIG,

[1] *CJCSI 6211.02B*, July 2003, page A-7, A8.

prior to connecting the voice telecommunications equipment to the DSN. The IATP is equivalent to the *ST&E Plan*.

IATT (Information Assurance Test Team).

ICTO (Interim Certification To Operate).

IO (Interoperability).

ISSO (Information System Security Officer).

JIC (Joint Interoperability Certification). The acquiring or sponsoring activity shall submit DSN voice telecommunications equipment to DISA for JIC processing. Either DISA JITC or AFIWC will test the DSN voice telecommunications equipment with acquiring or sponsoring activity sponsorship and involvement.

JITC (Joint Interoperability Test Command).

MUF (Military Unique Feature).

POC (Point Of Contact).

SSAA (System Security Authorization Agreements). A formal agreement among DAAs, CA, IT system user representative, and acquiring activity. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. The SSAAs shall document the operating agreements between DISN DAAs, CA, acquiring activity, and users of DSN. The SSAAs shall contain a record of any changes made to the architecture, configuration, or security of DSN that may affect the accreditation status of the system. The SSAAs shall be used to verify DSN mission, environment, and architecture. It shall identify threats to DSN and document compliance with C&A security requirements.

SSM (Single System Manager). The Director, DISA, is responsible for acting as the DSN SSM by providing operational direction and management control of DSN.[2]

- Single systems management is a process used by DISA, in conjunction with the services, O&M activities, and life-cycle managers to perform DSN administration and network management. In the role of the DSN SSM, the Director of DISA delegates authority to the DSN PM to implement appropriate policies and practices to manage DSN operational system.
- The DSN SSM provides day-to-day planning, leadership, organization, and control of functions that support system operation.
- The DSN SSM ensures that all products connected to the DSN have been fully certified and accredited before providing the DSN user with the ATC.

[2] *CJCSI 6215.01B*, September 2001, enclosure G, page G-3, Paragraph 4.a. (1).

STIG (Security Technical Implementation Guide). The DSN STIG provides technical security policies, requirements, and implementation details for both security features required for DSN voice telecommunications equipment and implementation guides for operating voice telecommunications equipment by DoD components. The STIG supports lease or procurement, testing and operational implementation procedures, and assists DSN sites in meeting minimum requirements, standards, controls, and options for protecting telecommunications switch operations. The DSN STIG is used as guidance in ensuring that systems are configured to an acceptable level of security once deployed in the field; they serve as one of the several sources for security requirements for the DSN.

TSSI (Telecomm Switched Services Interoperability)

User Categories.

- **C2 Users.** Users who have a requirement for C2 communications, but do not meet criteria for the class of "Special C2 user." C2 users include any person (i.e.: regardless of the position in the chain-of-command) who issue or receive guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (i.e.: including combat support, administration, and logistics); whether said guidance or order is issued or effected during peacetime or wartime. There are two types of C2 users:

    1. Users approved by the Chairman of the Joint Chiefs of Staff, Combatant Commanders, Service, or DoD Agency for **Priority** and **Routine** precedence origination.
    2. DoD users having a military mission that might receive C2 calls for orders or direction at precedence above Routine, even though they do not have a C2 mission for issuing guidance or orders; therefore, these users must be served by switching facilities that provide the MUFs of the DSN.

- **Special C2 Users.** A special class of user who has access to the DSN for essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. The user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, other members of the Joint Chiefs of Staff, Service Chiefs, and Combatant Commanders. Specifically, these Special C2 Users are identified through one or more validation processes of the Chairman of the Joint Chiefs of Staff, Combatant Commanders, Service, or DoD Agency for **Flash** and **Flash Override** precedence origination.

- **Non-C2 Users.** DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirements to ever originate or receive C2 communications under the definitions of C2 and Special C2 Users. During a crisis or contingency, they may be denied access to the DSN. These users are provided access to the DSN for the benefit of the DoD.

VCAO (Voice Connection Approval Office). The VCAO is established and maintained as an element within the DSN PM office. The VCAO acts as the staff element for DSN SSM to interact with DoD components to achieve DSN connection approval of telecommunications products. The VCAO coordinates IA testing and JIC testing for the DSN.

- IA Testing—this testing will normally be performed by members of DISA GES engineering staff. This testing will take place at either JITC, Ft. Huachuca, Arizona, or the Air Force Information Warfare Center (AFIWC), San Antonio, Texas.
- JIC Testing—this testing will normally be performed by members of the engineering staff located at either JITC, Ft. Huachuca, Arizona or the Air Force Information Warfare Center, San Antonio, Texas.

APPENDIX B: CONNECTION TEAM ELEMENTS

A. Voice Connection Approval Office (VCAO)

The VCAO is the focal point for the following DSN management activities.

- JITC IO and IA test requests, requirements, scheduling, and Approved Products List management for the DSN.
- DSN ATC request processing, approval, and notification.
- Local site DITSCAP assistance and monitoring agent for the DSN.

Sponsorship

All requests for DSN testing at the JITC require the support of a Government sponsor. Any Government employee, with either acquisition or management level responsibilities for the solution requested for testing, can sponsor these tests. Upon receipt of an application for testing, the sponsorship POC information provided on the application will be verified prior to the final processing of the request.

STIG Compliance

STIG Compliance is a new requirement for testing of solutions at the JITC. Compliance with all current STIGs, that are applicable to a solution being submitted for testing, is verified during a Solutions Scheduled Lab Set Up period. The determination on exactly what STIGs are applicable to a given solution can be determined during the JITC IA In-brief. An applicant (vendor/sponsor) can determine what STIGs are applicable prior to that by contacting either ns534-web@ncr.disa.mil or fso_spt@ritchie.disa.mil.

Vendor Support

Vendor Support is not a requirement for solution certification testing at the JITC, although it is preferred. If a sponsor decides to test without vendor support for a solution, they are responsible for coordinating system setup, lab fees, and personnel to support the actual testing. (If a Government sponsor has difficulty locating a vendor POC for a solution, please contact the VCAO via email at ns534-web@ncr.disa.mil. The VCAO maintains a list of vendor POCs, for the majority of current Government solution vendors, which can be provided upon request.)

Scheduling

The DoD Telecom Switched Services Interoperability (TSSI) scheduling meetings are normally held on a bi-weekly basis. These meetings are the only times that either IO or

IA testing at JITC can be officially scheduled. The results of a TSSI scheduling meetings are posted on the JITC web page on the day following the meeting. (Access http://jitc.fhu.disa.mil/tssi/schedule.html.)

Solution Changes/Updates/Regression

All applicants are required to send all notifications of solution changes, requests for regression tests, or requests for schedule changes to ns534-web@ncr.disa.mil. Upon receipt of a request for change, sponsor authorization of the change will be verified. After verification is complete, a change-request-notification will be sent to all involved with the test. The change request will then be added to the agenda for the next TSSI scheduling meeting for discussion.

B. Interoperability Testing – JIC Test Process

To meet the DSN APL requirements, the following provides an overview of the JIC test process.

1. Once the JITC AO receives a VCAO Test Submittal Form with a VCAO Tracking Number assigned, the proposed solution(s) are analyzed against the DoD Voice Networks GSCRs for technical requirements. The AO will contact the DoD sponsor of the proposed test for implementation requirements, and maintain contact with the sponsor throughout the testing process for updates and changes. The AO will also contact the vendor for technical documentation, Letters of Compliance, and to discuss funding requirements. The AO will maintain contact with the vendor throughout the testing process for updates and/or changes. The AOs can be reached at DSN (312) 869-8575/5041/5164.

2. The JITC AO will attend the DoD TSSI scheduling meeting conducted by the VCAO along with the IA team to schedule testing at the Joint Interoperability Test Command, Ft. Huachuca, AZ.

3. The JITC AO is the POC for coordination with the vendor for equipment delivery and setup at the Joint Interoperability Test Command, Ft. Huachuca, AZ.

4. The JITC AO monitors JIC testing. Once all JIC testing requirements are met, an "Intent to Certify" email is sent to inform the DOD sponsor and product vendor that the systems have passed JITC tests, but the official certification letters have not been published. Once reviewed, approved, and signed, a Joint Interoperability Certification memorandum will be published and posted on the TSSI website (http://jitc.fhu.disa.mil/tssi/).

5. For more information about DoD policy for JITC testing, refer to: http://jitc.fhu.disa.mil/tssi/dodpolicydocs.html.

6. For more information about JITC requirements and testing documents, refer to: http://jitc.fhu.disa.mil/tssi/reqtstdocs.html.

C. Information Assurance (IA) Testing – Rules of Engagement

1. Solution test support personnel are required to attend the IA in-brief prior to the test schedule being finalized. Solution-capable support personnel are to be onsite during Phase I only. During Phase I, the applicant must demonstrate the full functionality of their solution to the IA testing personnel. For the Phase II part of the testing, the applicant will provide contact information for phone support in the event that a system component is unresponsive, unreachable, or unable to be tested.

2. There is no guaranteed length of time for IA testing. The length of testing depends on the complexity of the system being tested and the discretion of the Test Lead. Likewise, there is no guarantee for the length of time required for the scheduling of a system for testing. Scheduling of a system for testing is dependent upon availability, testing schedules, and at the discretion of the assigned on-site IA Test Lead.

3. The test teams reserve the right to have full access to any system being submitted for testing. Refusal to comply with a request of the test teams during the testing of a system in a timely manner (i.e., additional system access, additional system information, additional configuration data, etc.) may result in early termination of testing. In such cases, the system will have to be resubmitted to JITC for testing at a later date.

4. The applicant support personnel are responsible to contacting the IA team if unable to be present at the appointed time and date. If the applicant cannot be present or will not be prepared for IA testing, they are responsible for advising the IA team at least five business days in advance. With ample notice, the IA team will make a liberal attempt to reschedule the testing. If the applicant fails to provide notice at least five business days prior to the scheduled testing, re-scheduling for the system test will default to the end of the IA test schedule.

5. Once testing has officially begun on a system, the configuration of that system cannot be changed unless specifically directed by the test teams. This is to ensure that a consistent system configuration is maintained throughout the entire testing process.

APPENDIX C: FUTURE MODEL OF DSN ATC REQUEST PROCESS

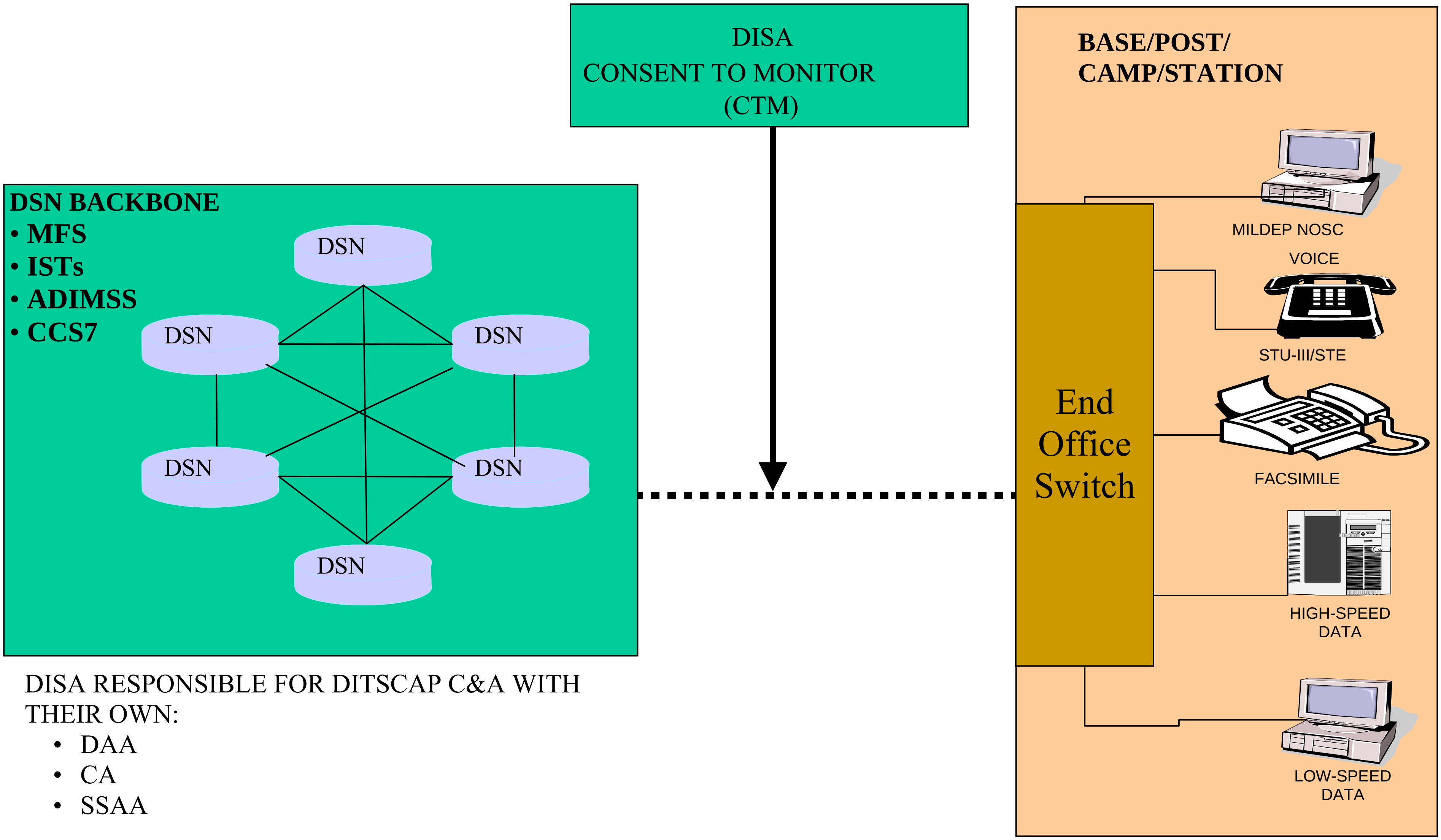
FUTURE MODEL of DSN CONNECTION APPROVAL (AUTOMATED SNAP/CAP)

The vision of the *NIPRNet System/Network Approval Process (SNAP)* will maintain quality support for the DoD customer (i.e.: user level, DoD Component Headquarters, IA Community, and Senior Leadership) through automation. The primary goal will provide the customer the ability to access a single, highly available and secure website https://cap.nipr.mil/ to enter information for DISN CAP, DATMS-U, and IP Core, OSD GIG Commercial Internet Waiver Process and Ports, and the Protocols and Services Adjudication Process Application (PPSAPA).

SNAP will have the ability to leverage existing hardware, software and software licenses, and the customer's familiarity with the website. Those DoD components familiar with the data network CAP will find it relatively easy to transition to the same process for DSN Voice Network; the SNAP/CAP model. See the following diagram.

This automated model will include DSN voice users in the future. The major difference will be that the data world uses CCSD numbers as database identifiers to track users while it is envisioned that the voice world will use a system based upon the switch Facility Identifier (FID) as the database identifier.

Note: Figure C-1 represents the current model of the DITSCAP process. This process will be moving to the SNAP in the future.



DISA
CONSENT TO MONITOR
(CTM)

DSN BACKBONE

- **MFS**
- **ISTs**
- **ADIMSS**
- **CCS7**

BASE/POST/
CAMP/STATION

End Office Switch

DISA RESPONSIBLE FOR DITSCAP C&A WITH THEIR OWN:

- DAA
- CA
- SSAA

DOD COMPONENT RESPONSIBLE FOR LOCAL DITSCAP C&A WITH THEIR OWN:

- DAA
- CA
- SSAA

FIGURE C-1   SNAP/CAP MODEL

APPENDIX D: REFERENCES

CJCSI 6215.01B, 23 September 2001, Policy for DoD Voice Networks.

CJCSI 6211.02B, 31 July 2003, DISN Policy, Responsibilities, and Processes.

DoDI 8100.3, 16 January 2004, DoD Voice Networks.

DoDD 4630.5, January 2002, Interoperability and Supportability of Information Technology 9IT) AND National Security Systems (NSS).

DoDD 5100.35, 10 March 1998, Military Communications-Electronics Board (MCEB).

DoDI 5200.40, 30 December 1997, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

Public Law 104-106, "Subdivision E of the Clinger-Cohen Act of 1996," February 10, 1996 (formerly the Information Technology Management Reform Act of 1996.)

Public Law 107-314, December 2, 2002. Bob Stump National Defense Authorization Act for Fiscal Year 2003.