



Office, Director of Information
Systems for Command, Control,
Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

S: 15 August 2001
S: 31 January 2002

SAIS-IAS (380)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

1. References.

a. Defense Information Services Agency (DISA) Message, 021730ZNOV99, subject: DISN Unclassified But Sensitive Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP).

b. Army Message, 151800ZJUN00, subject: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP).

c. Department of Defense Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997.

d. Department of Defense Manual 8510.1-M, DITSCAP Application Manual, 31 July 2000.

e. Army Regulation (AR) 380-19, Information Systems Security, 27 February 1998.

f. Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Public Law No. 106-398, Subtitle G, Government Information Security Reform (GISR) (Sections 1061-1065 (2000) (NOTAL).

2. As both the CAP process and the GISR requirements rely heavily on certification and accreditation (C&A) to be accomplished, the purpose of this memorandum is twofold.

a. It is a reminder/update to Directors of Information Management (DOIMs) and Information Assurance Program Managers (IAPMs) that all installation campus area network (CAN) backbone infrastructures must be accredited by 15 Aug 01 (Refs a and b). It extends the deadline for accrediting organization-level local area networks (LAN), which are attached to the DOIM backbone, to 31 Jan 02.

SAIS-IAS (380)

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

b. It outlines initial Department of Defense (DoD) guidance to Commanders in Chief, Services, and Agencies (C/S/A) for meeting Subtitle G, Government Information Security Reform (GISR), requirements of the FY 2001 Defense Authorization Act (Ref f). Subtitle G, GISR, requires all government agencies to conduct annual Information Assurance (IA) program status reviews and independent audits of their IA programs, and report the results to the Office of Management and Budget (OMB).

3. **Connection Approval Process (CAP):** All post, camp, and station NIPRNET circuits (also referred to as Army Category I connections) must meet the NIPRNET CAP requirements before DISA will grant an authority to connect for that NIPRNET circuit. The CAP requirements are outlined in the DISA CAP Website (<http://cap.nipr.mil/>). A significant component of the CAP requirement is that the installation CAN backbone infrastructure that connects to the NIPRNET, and all systems connected to the CAN, to include tenant systems, be accredited before an Authority to Connect (ATC) is granted by DISA.

4. To ensure all Army post, camp, and station NIPRNET circuits meet the requirements for connection, and in accordance with (IAW) references a and b above, the DOIMs must accomplish the following actions by 15 Aug 01:

a. Accredite the CAN backbone infrastructure according to references c, d, and e above. As a minimum, the CAN backbone infrastructure accreditation includes the Army DISN Router Program (ADRP) router, switches, other routers, etc. that support and further connect the installation organizations and tenants serviced by the CAN. It also includes those DOIM hosts and critical systems/servers, which are under the DOIM control and are essential to the installation organization being able to fulfill its mission, e.g., main email servers. A diagram displaying what must be accredited by 15 Aug 01 is attached and also displayed on the DISC4 Information Assurance website (http://www.army.mil/disc4/organization/Info_assurance.html).

b. Accredite local area networks (LAN) and systems attached to the CAN (see diagram). The date for these accreditations is extended until 31 Jan 02. However, organizations with systems connected to the CAN backbone, to include tenant activities, will continue to accredit their systems IAW references c, d, and e and provide the accreditation documentation to the DOIM as a condition for connection to the CAN backbone. Major Command (MACOM) and Program Executive Office (PEO)/Program Manager (PM) Information Assurance Program Managers (IAPM) must report, on 15 Aug and 15 Nov 01, to the accreditation POC at paragraph 9, the percentage of completion of the accreditations for LANs/systems which are connected to the CAN backbone infrastructure but which are not part of the backbone. (Example: 100 systems connected; 60 percent granted approval to operate [ATO]; 25 percent granted an interim approval to operate [IATO]; 15 percent pending ATO/IATO.)

SAIS-IAS (380)

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

c. Ensure the Accreditation Information and Designated Approving Authority (DAA) Information sections of the CAP Data Template (<http://cap.nipr.mil/>) are updated with the most current accreditation status for the installation CAN backbone infrastructure (Category 1 NIPRNET connection). NOTE: If your organization has been operating under the blanket IATO authorized by HQDA in reference b, the installation CAN backbone infrastructure ATO must replace the HQDA blanket IATO by 15 Aug 01. The ASC CAP Manager, who is identified in paragraph 9, can provide assistance with completing and updating the CAP Data Template.

5. By 31 Jan 02, the following actions must be accomplished:

a. All LANs/systems connected to the installation CAN backbone infrastructure must be accredited. Failure to comply with this requirement shall constitute grounds for the DOIM to disconnect the system from the installation backbone. Non-Army tenants that cannot meet this accreditation requirement will be referred to the HQDA Accreditation POC identified in paragraph 9 below.

b. Provide the status of these accreditations (by percentage of completion) to the Accreditation POC at paragraph 9.

6. The connection approval process for NIPRNET circuits and the certification and accreditation requirements for information technology systems are on-going requirements. Installation DOIMs that have numerous systems connected to their backbones may have systems undergoing accreditation/reaccreditation continuously throughout any particular year. To address these changes in status, without having to constantly reaccredit the CAN backbone and modify the CAP status, installation accreditation authorities will conduct risk management analyses and make accreditation decisions for their posts, camps, or stations based on their installations' overall information assurance (IA) posture. These risk management analyses will follow the DITSCAP Phase 4, Post Accreditation requirements, as outlined in references c and d above.

7. Government Information Security Reform (GISR) Requirements: In an effort to ensure these IA activities are actually contributing to an improved security posture for the Federal Information Infrastructure (FII), Congress enacted Subtitle G, GISR, of the Defense Authorization Act for Fiscal Year 2001. Subtitle G mandates the Department of Defense and other federal agencies conduct annual reviews and selected evaluations of information systems and submit a report of results to the Office of Management and Budget (OMB).

a. Army will provide input to the Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C3I) Chief Information Officer (CIO) in

SAIS-IAS (380)

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

support of the DoD response to these new requirements. The proposed DoD plan, being created by a DoD led Integrated Process Team (IPT), will establish a mechanism to provide a corporate overview (C/S/A do not report separately) of DoD's current IA posture as it applies to Secret and Unclassified systems. The intelligence community Chief Information Officer (CIO) will address sensitive compartmented information (SCI) systems.

b. The mechanism has three major phased activities: Select, Control, and Evaluate. These activities determine the candidate information systems (IS) for developing the annual corporate IA posture, provide input to the existing assessment and evaluation processes, and analyze the information developed for an annual DoD GISR report. The Information Technology (IT) Registry (formerly the Y2K Database) will serve as the initial repository of IS eligible for review. There are about 1200 Army systems in the IT Registry. A DoD process for C/S/A reporting is being developed. The first iteration of the GISR requirements reporting process must be accomplished by the end of fiscal year (FY) 01. DoD expects to finalize the process by the end of Apr 01. If this is accomplished, Army will promulgate reporting requirements and timelines in the first week of May 01.

8. At present, DoD anticipates directing C/S/A to report on a random sample of 10 percent of the systems in the IT Registry for which they are responsible. Any Army organization that is a proponent for a system registered in the DoD IT Registry will be subject to examination. In addition, the DoD Inspector General (IG), supported by the U.S. Army Audit Agency (AAA), is tasked to conduct an independent audit of the program. Given the short time frame, the DoD IG has developed evaluation criteria and directed the AAA to audit 34 Army systems. AAA is in the process of contacting system owners and conducting in-briefings on the task. AAA anticipates having a draft audit report on the IA status of the 34 systems by 15 Jul 01 and must submit their results to the DoD IG by 1 Aug 01. DoD IG assessment and evaluation criteria are expected to be essentially similar to what the DoD IPT expects to publish by the end of Apr 01.

9. Points of contact are noted below:

a. HQDA Accreditation POCs are Mr. Albert Kondi, 703-604-7572, DSN 664, Albert.Kondi@hqda.army.mil, and Ms. Jeanne Medeiros-Williams, 703-601-0741, DSN 329, Jeanne.Medeiros-Williams@hqda.army.mil.

b. HQDA GISR POCs are LTC John Quigg, 703-604-8377, DSN 664, John.Quigg@hqda.army.mil, and Mr. Ronald Sturmer, 703-604-6870, DSN 664, Ronald.Sturmer@hqda.army.mil.

SAIS-IAS (380)

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

c. HQDA NIPRNET CAP POC is Mr. Bill Buzinski, 703-607-5888, DSN 327, William. Buzinski@hqda.army.mil.

d. ASC NIPRNET CAP Manager is Mr. Tom Lindholm, USANETA-Army Telecommunications Directorate (ATD), 520-538-1826, DSN 821, thomas.lindholm@hqasc.army.mil.

Encl
CAN Diagram



KIRK M. KRIST
COL, GS
Director, Information
Assurance

DISTRIBUTION:

DA, INSPECTOR GENERAL, ATTN: INFORMATION RESOURCE MANAGEMENT DIVISION, 2511 JEFFERSON DAVIS HWY, SUITE 12700, ARLINGTON, VA 22202-3912

DA, DEPUTY CHIEF OF STAFF FOR PERSONNEL, ATTN: DAPE-ZXI-AA, 200 STOVALL STREET, ALEXANDRIA, VA 22332-4000

PROGRAM EXECUTIVE OFFICER, AIR AND MISSILE DEFENSE, ATTN: SFAE-AMD-IO, 215 WYNN DRIVE, SUITE 201, HUNTSVILLE, AL 35807-3801

PROGRAM EXECUTIVE OFFICER, AVIATION, ATTN: SFAE-AV, BUILDING 5300, REDSTONE ARSENAL, AL 35898-5000

PROGRAM EXECUTIVE OFFICER, COMMAND, CONTROL, AND COMMUNICATIONS SYSTEMS, ATTN: SFAE-C3S-HTI, FORT MONMOUTH, NJ 07703-5501

PROGRAM EXECUTIVE OFFICER, GROUND COMBAT SUPPORT SYSTEM, ATTN: SFAE-GCSS-W, WARREN, MI 48397-5000

PROGRAM EXECUTIVE OFFICER, INTELLIGENCE, ELECTRONIC WARFARE & SENSORS, ATTN: SFAE-IEWS, FORT MONMOUTH, NJ 07703-5501

PROGRAM EXECUTIVE OFFICER, STANDARD ARMY MANAGEMENT INFORMATION SYSTEMS, ATTN: SFAE-PS, 9350 HALL ROAD, SUITE 142, FORT BELVOIR, VA 22060-5526

PROGRAM EXECUTIVE OFFICER, TACTICAL MISSILE, ATTN: SFAW-MSL-I, REDSTONE ARSENAL, AL 35898-8000

COMMANDER, FORCES COMMAND, ATTN: AFCI-JI, 1777 HARDEE AVE SW., FORT McPHERSON, GA 30330-1062

COMMANDER, EIGHTH ARMY, HEADQUARTERS, US ARMY GARRISON, ATTN: EAIM-C-C4, UNIT #15236, APO AP 96205-0009

SAIS-IAS (380)

SUBJECT: Army Nonsecure Internet Protocol Router Network (NIPRNET) Connection Approval Process (CAP) Update and Government Information Security Reform (GISR) Requirements Notification

COMMANDER, U.S. ARMY PACIFIC, HEADQUARTERS, FORT SHAFTER, HI
96858-5100

COMMANDER, U.S. ARMY SOUTH, ATTN: DCSIM SOIM-IT-IA, P.O. BOX 34000,
FORT BUCHANAN, PR 00934-3400

COMMANDER, U.S. ARMY EUROPE AND SEVENTH ARMY, ATTN: AEAIM, UNIT
29351, APO AE 09014

COMMANDER, U.S. ARMY TEST AND EVALUATION COMMAND, ATTN:
INFORMATION ASSURANCE PROGRAM MANAGER, PARK CENTER IV, 4501
FORD AVENUE, ALEXANDRIA, VA 22302-1458

COMMANDER, U.S. ARMY MATERIEL COMMAND, ATTN: AMCIO-F, 5001
EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

COMMANDER, U.S. ARMY AVIATION AND MISSILE COMMAND, ATTN: AMSMI,
REDSTONE ARSENAL, AL 35898-5160

COMMANDER, U.S. ARMY SIGNAL COMMAND, ATTN: AFSC-PLM, FORT
HUACHUCA, AZ 85613-5000

COMMANDER, U.S. ARMY TRAINING AND DOCTRINE COMMAND, ATTN: ATIM-I,
BUILDING 100, FORT MONROE, VA 23651-5000

COMMANDER, U.S. ARMY LOGISTICS INTEGRATION AGENCY, 54 M. AVENUE,
SUITE 4, NEW CUMBERLAND, PA 17070-5007

COMMANDER, MEDICAL COMMAND, 2050 WORTH ROAD, SUITE 13, FORT SAM
HOUSTON, TX 78234

COMMANDER, U.S. ARMY WAR COLLEGE, ATTN: AWCC-SAS-CR, 122 FORBES
AVE, CARLISLE, PA 17013-5219

COMMANDER, U.S. ARMY INTELLIGENCE AND SECURITY COMMAND, ATTN:
INFORMATION ASSURANCE PROGRAM MANAGER, 8825 BEULAH STREET,
FORT BELVOIR, VA 22060-5246

COMMANDER, MILITARY TRAFFIC MANAGEMENT COMMAND, 200 STOVALL
STREET, ALEXANDRIA, VA 22332-5000

COMMANDER, U.S. TOTAL ARMY PERSONNEL COMMAND, ATTN: TAPC-ZA, 200
STOVALL STREET, ALEXANDRIA, VA 22332-4000

U.S. ARMY RESERVE COMMAND, ATTN: AFRC-CII, 1401 DESHLER STREET SW,
FORT MCPHERSON, GA 30330-2000

DIRECTOR ARMY NATIONAL GUARD, ATTN: NGB-ARZ, 2500 ARMY PENTAGON,
ROOM 2E408, WASHINGTON, D.C. 20310-2500

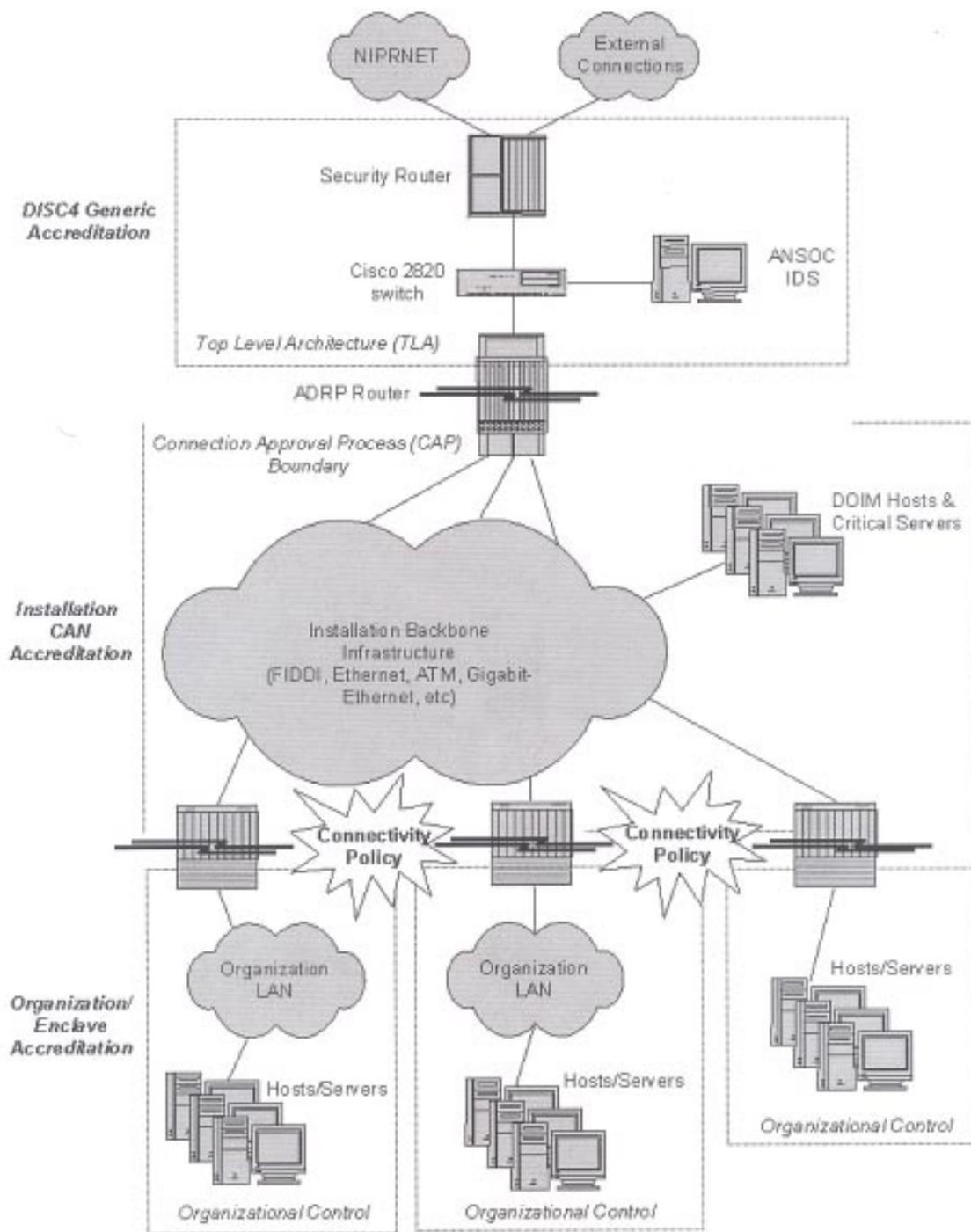


Figure 1. ICAN Accreditation Boundary