



---

JOINT INTEROPERABILITY TEST COMMAND

---



INFORMATION  
TECHNOLOGY  
SECURITY USER  
INSTRUCTION



JUNE 2007  
Supersedes edition of  
March 2007



**JOINT INTEROPERABILITY TEST COMMAND  
FORT HUACHUCA, ARIZONA 85670-2798**

JITC Instruction 240-110-03\*

JUN 21 2007

**SECURITY**

**Information Technology  
Security User Instruction**

1. **Purpose.** This instruction establishes the general user responsibilities and procedures for the secure and efficient operation of the Joint Interoperability Test Command (JITC) Automated Information Systems (AISs) in accordance with (IAW) Department of Defense (DoD) security policies and Defense Information Systems Agency (DISA) and JITC instructions. It covers procedures and provides references to additional information sources.
2. **Applicability.** This instruction applies to the use of the JITC DISA Network (DISANet), other JITC AIS, laboratories, and testbeds at JITC Fort Huachuca and JITC Indian Head. Provisions applicable to specific AISs are found in the systems' Laboratories Books.
3. **Authority.** DoD Directive (DoDD) 8500.1, Information Assurance (IA), 24 October 2002.
4. **References.**
  - 4.1 DoD 5200.1R, Information Security Program, January 1997.
  - 4.2 DoD 5200.2R, Personnel Security Program, January 1987, changes: 12 February 1990, 14 July 1993, and 23 February 1996.
  - 4.3 DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005.
  - 4.4 DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
  - 4.5 DISAI 240-110-8, Information Security Program, 24 June 1996.
  - 4.6 DISAI 630-225-7, Information Services, Internet, Extranet, and World Wide Web, 28 August 2003.

---

\* This Instruction supersedes JITCI 240-110-03, dated March 2007  
OPR: JT2B  
DIST: All JITC Civilian, Military, and Contractor Personnel

4.7 DISAI 630-230-19, Automatic Data Processing - Information Systems Security Program, 9 July 1996.

4.8 DISA - Western Hemisphere Security Handbook, Version 3, 1 December 2000.

4.9 DISA - Universal Serial Bus (USB) Checklist for Sharing Peripherals Across the Network (SPAN) Security Technical Implementation Guide, Version 1 Release 1 6, January 2006

5. **Responsibilities.** Areas of responsibility are listed in C1.4.

6. **Delegation of Authority.** The JITC Commander has delegated to the Information Assurance Manager the responsibility of DISAI implementation/compliance and the establishment of the JITC Information Assurance program.

  
LUANNE OVERSTREET  
Acting Commander

SUMMARY OF SIGNIFICANT CHANGES. Added reference 4.3. Corrected information in paragraph C1.4.1. Clarified Information Technology Access Requirements in paragraph C2.2. Added Information Assurance Technical Level position information as paragraph C3.3 and renumbered the rest of chapter 3 paragraphs. Updated USB information in supplement 5.

## TABLE OF CONTENTS

	<u>Page</u>
<b><u>BASIC INSTRUCTION</u></b>	
1. Purpose	i
2. Applicability	i
3. Authority	i
4. References	i
5. Responsibilities	ii
6. Delegation of Authority	ii
7. Acronyms and Definitions	vi
<b>C1 <u>CHAPTER 1. SECURITY ORGANIZATION</u></b>	1-1
C1.1 GOVERNMENT CIVILIAN AND MILITARY PERSONNEL	1-1
C1.2 CONTRACTOR PERSONNEL	1-1
C1.3 IT SECURITY MANAGEMENT	1-1
C1.4 RESPONSIBILITIES	1-1
C1.4.1 JITC Security Manager	1-1
C1.4.2 JITC Information Assurance Manager	1-1
C1.4.3 Information Assurance Officer	1-2
C1.4.4 System Administrator (SA)	1-3
C1.4.5 Individual User	1-3
<b>C2 <u>CHAPTER 2. JITC GENERAL AIS PROVISIONS</u></b>	2-1
C2.1 PASSWORDS	2-1
C2.2 INFORMATION TECHNOLOGY ACCESS REQUIREMENTS	2-1
C2.3 INFORMATION ASSURANCE TECHNICAL/MANAGER LEVELS POSITION DESIGNATIONS	2-1
C2.4 IS CONTINGENCY PLAN	2-2
C2.5 FREEWARE/SHAREWARE	2-2
C2.6 COPYRIGHTED MATERIAL	2-2

## TABLE OF CONTENTS

	<b><u>Page</u></b>
C2.7 DATA BACKUP RESPONSIBILITIES	2-2
C2.8 LOCKING THE WORKSTATION	2-2
C2.9 COMPUTER VIRUSES	2-3
C2.10 DISANET	2-4
C2.10.1 Messaging Hints for Efficient Use of E-mail	2-4
C2.10.2 E-mail Usage	2-5
C2.10.3 E-mail Prohibitions	2-5
C2.10.4 Internet Access and Activity	2-6
C2.10.5 Software on DISANet	2-7
C2.10.6 Temporary E-mail Accounts	2-7
C2.10.7 Dial-in Access	2-7
C2.11 AUTOMATED INFORMATION SYSTEMS, LABS, AND TESTBEDS	2-7
C2.12 USE OF PORTABLE ELECTRONIC DEVICES WITHIN JITC FORT HUACHUCA ENCLAVE	2-7
<b>C3 <u>CHAPTER 3. JITC AIS ACCESS REQUEST</u></b>	<b>3-1</b>
C3.1 FORM 40	3-1
C3.2 DD FORM 2875	3-1
C3.3 JITC INFORMATION ASSURANCE MANAGER (IAM) RETAINS COMPLETED FORMS	3-1
<b>C4 <u>CHAPTER 4. VISITORS TO JITC</u></b>	<b>4-1</b>
C4.1 JITC HOST	4-1
C4.2 IT EQUIPMENT	4-1
C4.3 VISITOR'S ACCESS TO JITC IT EQUIPMENT	4-1
C4.4 VISITOR'S OUT-PROCESSING	4-2

## TABLE OF CONTENTS

	<u>Page</u>
<b>C5 <u>CHAPTER 5. JITC PERSONNEL VISITING OTHER LOCATIONS</u></b>	5-1
C5.1 HAND RECEIPT	5-1
C5.2 CLASSIFIED MATERIAL	5-1
C5.3 PROTECTION OF IT EQUIPMENT	5-1
<b>C6 <u>CHAPTER 6. ADDITIONAL SOURCES OF IT SECURITY INFORMATION</u></b>	6-1
 <b>SUPPLEMENTS</b>	
1. DEFENSE INFORMATION SYSTEMS AGENCY (DISA) DIRECTOR'S POLICY LETTERS	S1-1
2. JOINT INTEROPERABILITY TEST COMMAND (JITC) POLICY ON ANALYSIS AND INCIDENT HANDLING IN CASE OF INTERNET SERVICES ACCESS POLICY VIOLATIONS	S2-1
3. DEFENSE INFORMATION SYSTEMS AGENCY (DISA) POLICY ON ACCOUNT PASSWORDS	S3-1
4. TRANSFER OF UNCLASSIFIED DATA ON A CLASSIFIED SYSTEM TO UNCLASSIFIED MEDIA	S4-1
5. DEFENSE INFORMATION SYSTEMS AGENCY (DISA) POLICY ON UNIVERSAL SERIAL BUS	S5-1

## LIST OF TABLES

1. Locking the Workstation	2-3
----------------------------	-----

## ACRONYMS AND DEFINITIONS

### Acronyms

AIS	Automated Information System
BI	Background Investigation
DCRA	Derivative Classification Review Agent
DISA	Defense Information Systems Agency
DISAI	DISA Instruction
DISANet	DISA Network
DNACI	DoD National Agency Check Plus Written Inquiry
DoD	Department of Defense
E-mail	Electronic Mail
GDS	Global Directory Services Lab
GSA	General Services Administration
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAT	Information Assurance Technical (Level categories)
IAW	In Accordance With
IS	Information Systems
IT	Information Technology
JITC	Joint Interoperability Test Command
NACI	National Agency Check Plus Written Inquiry
NDA	Non-Disclosure Agreement
NSO	Network Security Officer
PC	Personal Computer
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PKE	Public Key Enabled
POC	Point of Contact
SA	System Administrator
SCIF	Sensitive Compartmented Information Facility
SIPRNet	SECRET Internet Protocol Router Network
STIG	Security Technical Implementation Guide

URL                      Uniform Resource Locator

## Definitions

**Automated Information System** - A configuration of computer hardware, software, and/or firmware assembled to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

**Basic Internet Services** – Internet services refer to the general Internet and Intranet capabilities provided to the typical JITC user. These services are provided within established JITC resources and typically include a web browser, email capabilities to Internet and Intranet addresses and other services. Internet services are predominantly user-level services.

**Contingency Plan** - Plan maintained for emergency response, backup operations, and post-disaster recovery for an automated information system, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

**Enclave** - A network under the operational control and authority of a single organization with the responsibility to define and implement security controls.

- A group of one or more security domains that typically share close physical proximity and that can have a clearly defined perimeter. Within DoD this could be the case of a tenant activity located on a base controlled by another organization. The tenant activity will be expected to have a firewall at the perimeter of its network “enclave,” and additional internal firewalls to separate different security domains.

**Freeware** - Software that the author distributes freely, with no expectation of compensation.

**Information Systems** - The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (*Joint Pub 6-0*).

**Malicious Code** - Code designed with a malicious intent to deny, destroy, modify, or impede system configuration, programs, data files, or routines. Causes unwanted modification or destruction of data. It can also steal data, allow unauthorized access, and exploit/damage an Information System (IS) or entire network. Includes Trojan horses, bombs, worms, and viruses.

**Malicious Logic** - Hardware, software, or firmware intentionally included in an Information System (IS) for an unauthorized purpose.

**User** - In automated information systems, a person or process accessing an automated information system by direct connection (e.g., via terminals), or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

**Virus** - A computer program usually hidden within another seemingly innocuous program that produces copies of itself, often by inserting itself into other programs, and that usually performs a malicious action (such as destroying data).

## C1. CHAPTER 1. SECURITY ORGANIZATION

The Joint Interoperability Test Command (JITC) Information Technology (IT) security structure is designed to facilitate manageability and efficiency. It emphasizes individual user security awareness and responsibility.

**C1.1 Government Civilian and Military Personnel.** The JITC Security Office is the controlling organization for security matters concerning Federal Government civilian employees and military members supporting JITC. If there are general security questions or concerns, contact the Security Manager at 520.538.5573 (DSN 879), the Security Office at 520.538.5200 (DSN 879), or 520. 538.4242 (DSN 879). For JITC Indian Head contact the Security Manager at 301.744.2871 (DSN 354).

**C1.2 Contractor Personnel.** JITC contractors also have company-based security programs. In addition to Federal Government requirements, contractor personnel are also governed by their respective company security policies. A key contractor responsibility is guarding company proprietary data. In addition, JITC in-house projects may have numerous subcontractors, each of which may require Non-Disclosure Agreements (NDAs). It is vitally important that NDAs be respected and followed. If any questions arise about Conflict of Interest, or if there are general security questions or concerns, contact the respective company management, JITC management, or Defense Information Systems Agency (DISA) Field Security Operations Division.

### C1.3 IT Security Management.

C1.3.1 The JITC Commander has appointed an Information Assurance Manager (IAM) and an Alternate IAM at each JITC Facility to be the Commander's principal advisors in the area of IT Security.

C1.3.2 The JITC IAM has appointed Information Assurance Officers (IAOs) for each JITC Lab or group of like Automated Information Systems (AISs) to control processing and act as an immediate point of contact (POC) for IT-related security matters.

### C1.4 Responsibilities.

C1.4.1 **JITC Security Officer.** The JITC Security Officer is responsible for:

C1.4.1.1 Informing personnel of any security deficiencies that require individual corrective action.

C1.4.1.2 On a recurring basis, reminding personnel of their continuing responsibility to safeguard sensitive information and that unauthorized disclosure of sensitive information violates DoD regulations and contractual obligations, and is punishable under provisions of Federal criminal statutes.

C1.4.1.3 Ensuring users who have possession or knowledge of an element or item of sensitive information are informed that they are responsible for determining whether a prospective

recipient of the information is an authorized person and that they are required to advise the recipient of the information classification.

C1.4.1.4 The JITC Security Officer is responsible for JITC physical security and for ensuring government regulations and sound security practices are followed.

C1.4.2 **JITC Information Assurance Manager.** The JITC IAM is responsible for:

C1.4.2.1 Providing staff oversight of the IAOs.

C1.4.2.2 Acting as the principal advisor to the Commander on IT security matters.

C1.4.2.3 Evaluating, from a security perspective, all changes to systems/networks, including approval of network connectivity.

C1.4.2.4 Working with the JITC Security Manager to ensure security-related incidents and violations are immediately reported, properly investigated, and correctly resolved.

C1.4.2.5 On a regular basis, ensuring all IAOs and SAs receive the necessary technical and IA training, education, and certification to carry out their IA duties.

C1.4.2.6 Additional IAM responsibilities are defined in DISA Information Systems Security Program, DISAI 630-230-19, paragraph C1.8.1.

C1.4.3 **Information Assurance Officer.** The IAO is responsible for:

C1.4.3.1 Acting as the primary POC on system IT security matters.

C1.4.3.2 Designating the personnel authorized access to the AIS.

C1.4.3.3 Conducting reviews, at least annually, to determine compliance with this instruction and appropriate regulations.

C1.4.3.4 Reporting actual and possible unauthorized disclosures and security incidents to the JITC Security Manager.

C1.4.3.5 Maintaining logs and rosters associated with the AIS.

C1.4.3.6 Establishing and maintaining a system for the control of log-on user names, passwords, permissions, access areas, and other critical resources.

C1.4.3.7 Conducting security monitoring of processes on the computer systems to detect, identify, and prevent intentional and unintentional violations of computer security.

C1.4.3.8 Reviewing all configuration changes and system component changes or modifications to ensure the security is not compromised.

C1.4.3.9 Ensuring their system(s) SAs receive the necessary technical and IA training, education, and certification to carry out their IA duties.

C1.4.3.10 Additional IAO responsibilities are defined in DISA Information Systems Security Program, DISAI 630-230-19, paragraph C1.8.2.

C1.4.4 **System Administrator (SA).** The AIS SA is responsible for:

C1.4.4.1 Training of system personnel in individual responsibilities, including IA.

C1.4.4.2 Day-to-day operations of AIS.

C1.4.4.3 Obtaining permission from the JITC IAM to connect a new or modified system to one of the networks.

C1.4.4.4 Application of the provisions of this instruction and the JITC Contingency Plan.

C1.4.4.5 Additional SA responsibilities are defined in DISA Information Systems Security Program, DISAI 630-230-19, paragraph C1.9.4.

C1.4.5 **Individual User.** Any individual who uses a JITC AIS should be aware of the information control procedures for that AIS and should obtain additional information or procedure clarification from the system IAO, if necessary. All users are responsible for:

C1.4.5.1 Reporting actual and suspected security incidents to the IAO. This includes warnings or notices not normally displayed by the system during normal operations.

C1.4.5.2 Using only their user name and assigned password when logging onto any JITC AIS.

C1.4.5.3 Not disclosing their user name or password to other individuals.

C1.4.5.4 Not logging on with their own user name and password and letting another individual use the account afterwards.

C1.4.5.5 Not performing or attempting to perform unauthorized modifications to the system hardware or software.

C1.4.5.6 Not moving hardware or altering communications connections without prior approval from the SA/Network Security Officer (NSO).

C1.4.5.7 Scanning all diskettes for viruses before using. See paragraph C2.8.2.

C1.4.5.8 Operating the system reliably and using the system only as configured by the SA.

C1.4.5.9 Not attempting to access files or data, or use operating systems programs, except as specifically designed or authorized.

C1.4.5.10 Not leaving terminals signed on and unattended.

C1.4.5.11 Notifying the IAO when access to the AIS is no longer required.

C1.4.5.12 Complying with all provisions of this instruction and other JITC and DISA security and IA policies.

## **C2. CHAPTER 2. JITC GENERAL AIS PROVISIONS**

### **C2.1 Passwords.**

C2.1.1 The DISA Password Policy is contained in supplement 3 of this instruction.

C2.1.2 The user should apply the principles of the DISA Password Policy to all passwords, including systems not on the DISANet. Check with the system's SA if a system will not allow special characters.

### **C2.2 Information Technology Access Requirements.**

C2.2.1 Information Technology (IT) access requirements are explained in chapter 3 and appendix 10 of DoD 5200.2R. Briefly, IT I access requires a Background Investigation (BI). IT II access requires a National Agency Check Plus Written Inquiry (NACI) or DoD National Agency Check Plus Written Inquiry (DNACI).

C2.2.2 At a minimum, Joint Interoperability Test Command (JITC) users will require IT II. IT III is not currently valid for use within Defense Information Systems Agency (DISA).

C2.2.3 Individuals with the capability to bypass security, such as some of the Information Assurance Officers (IAO)s or System Administrators (SA)s, will require IT I. This is an absolute requirement on all administrative systems. However, this requirement is generally waived on test systems. Frequently, in order to accomplish test functions, all personnel will require SA type access on test systems.

C2.2.4 The JITC Information Assurance Manager (IAM) will identify those individuals who will be designated IT I.

**C2.3 Information Assurance Technical/Manager Levels Position Designations.** The three levels of the Information Assurance (IA) workforce structure are: the computing environment, Level I; the Network, Level II; and the Enclave, Level III. These levels apply to both the IA Technical (IAT) and the IA Manager (IAM) positions.

C2.3.1 The IAT Levels position designations are explained in chapter 3 of DoD 8570.01-M. These positions require a certification listed in table AP3.T1 from an organization listed in table AP3.T2. Personnel without a certification will not be allowed privileged access.

C2.3.2 The IAM Levels position designations are explained in chapter 4 of DoD 8570.01-M. These positions require a certification listed in table AP3.T1 from an organization listed in table AP3.T2. Personnel without a certification will not be allowed privileged access. The IAM positions are called IA Officers (IAO) and Network Security Officers (NSO) at JITC.

C2.3.3 The JITC Information Assurance Manager (IAM) will appoint personnel to the IAT and IAM positions.

**C2.4 IS Contingency Plan.** This plan details actions required in response to emergencies and disasters. If the user works in one of the test labs, the lab SA has a copy in the system's Lab Book. Other users may obtain a copy to review from the JITC Library.

**C2.5 Freeware/Shareware.** These types of programs must be approved by the JITC IAM before being downloaded from the Internet and introduced into a DISANet JITC Automated Information System (AIS). Network Operations will perform the installation of approved programs for any installation required of a DISANet system.. JITC Labs/Systems will follow their accredited SOP if freeware/shareware installation is needed for their accredited AIS.

**C2.6 Copyrighted Material.** Illegal copies of software are not permitted on any JITC AIS. Copies of copyrighted material cannot be made without written permission of the copyright holder or authorized agent.

### **C2.7 Data Backup Responsibilities.**

**C2.7.1** Network Operations is responsible for backing up the DISANet server disk drives, and does so daily using tape backup units. Network Operations will restore data from the backup tapes to the servers in those instances where data is destroyed or becomes corrupt. Backed-up data includes user data, group directory data, system state data, and electronic mail (e-mail) data. DISANet users are expected to backup their own workstation hard drive(s). The Security Technical Implementation Guide (STIG) requires that the automatic timed backup features available in most standard DISANet applications be turned off.

**C2.7.2** Test Support and Lab SAs are responsible for implementing backup procedures for their associated AISs and documenting them in their Contingency Plan.

**C2.8 Locking the Workstation.** Never leave the workstation unattended or unsecured while logged on to the DISANet. Doing so allows an unauthorized person access to all the applications and information on the workstation. If the user needs to leave the desk while working on the DISANet, the user remains logged on and secure by locking the workstation. This may be done with applications open. Procedures for locking the workstation are contained in table 1.

**NOTE:** Users must understand that if a workstation is locked and the owner is not present when help desk or other service personnel arrive to work on it, the resolution of reported problems may be seriously delayed. If users are expecting a visit from Service Desk personnel, and they will be away from their workstation, they should log off completely.

**Table 1. Locking the Workstation**

FUNCTION	PROCEDURE
Locking the Workstation	Remove the Common Access Card (CAC) from the CAC Reader or
	Press CTRL+ALT+DELETE, holding down all three keys at once, release, and then select the Lock Workstation button.
Unlocking the Workstation	Place CAC in the CAC Reader and enter the pin number or
	Press CTRL+ALT+DELETE, holding down all three keys at once, release, enter the password, and press enter.
	The user is returned to the screen last used before locking the workstation.

Although the user is supposed to lock the workstation when leaving the desk, one will probably forget to do so from time to time. For that reason, the workstation will automatically lock after fifteen minutes.

**C2.9 Computer Viruses.** Each workstation on DISANet has computer virus detection and removal software that will run automatically each day. This automatic and comprehensive scan will detect and automatically clean viruses that may be infecting the workstation. Scanning the hard disk may take a couple of minutes to complete and will depend on the amount of data to be scanned. DISA Instruction 630-230-19 directs that DISA employees are responsible for complying with the agency's policies and procedures to protect the DISANet from computer viruses. This policy also dictates it will be considered a MAJOR SECURITY VIOLATION if an employee deliberately introduces malicious code into agency workstations and/or networks.

C2.9.1 Auto-Protect is loaded when the user logons and it runs in the background. The Norton Auto-Protect icon appears on the taskbar. Norton automatically checks programs and floppy disks at time of use and all files as they are opened.

C2.9.2 Norton AntiVirus will automatically scan the workstation hard drives once a day. If the user wants to manually execute Norton to scan the hard disk(s) or diskette(s), it is available on the Start menu in Programs, Norton AntiVirus Corporate Edition folder. To manually check workstation/diskette(s) for viruses:

C2.9.2.1 Click on the Norton AntiVirus icon.

C2.9.2.2 In the Norton AntiVirus main window, click on Scan, click on Scan a Floppy Disk or Scan Computer, and check the drive or drives to scan in the drives list box.

C2.9.2.3 Click the Scan button.

C2.9.3 If Norton AntiVirus detects a virus during a manual scan, it will give two options: Repair or Delete.

C2.9.3.1 Repair - Eliminates the virus and returns the infected file or boot record to its original state.

C2.9.3.2 Delete - Eliminates the virus by deleting the infected file.

C2.9.4 To ensure the antivirus software can identify viruses as they are introduced, Network Operations will periodically stage virus definition files for loading on the user workstations; the virus definition files are loaded at user logon. For this reason, it is mandatory that users log off at least once a day.

C2.9.5 Any occurrence of virus detection will be reported to:

C2.9.5.1 For Fort Huachuca call the Service Desk at 520.538.5313 (DSN 879) and also Network Operations at 520.533.4808 (DSN 821) or 520.538.5160 (DSN 879) or 520.538.4274 (DSN 879).

C2.9.5.2 For Indian Head call the Service Desk at 301.744.2721 (DSN 354) and also Network Operations at 301.744.2638 (DSN 354).

C2.9.6 Any files received from outside JITC on transport media or downloaded from the Internet to any DISANet facility or connected workstation must be checked for viruses. This is true for all files. They might contain Word macro viruses or executables in the attachments.

C2.9.7 DoD's Norton AntiVirus software license allows military and government civilian employees to download (to .mil sites only) and install Norton AntiVirus on their home computers. Unfortunately, this does not extend to DoD contractors. Visit the Joint Task Force – Global Network Operations (JTF-GNO) at <https://www.jtfgno.mil> online site for details.

## C2.10 DISANet.

**C2.10.1 Messaging Hints for Efficient Use of E-mail.** Following are several hints that can significantly reduce the volume of traffic on our system. Limiting the number of addressees and limiting attachments can result in lighter loading across the system, and can reduce message storage volume, both on the network equipment and on the user's own workstation's hard disk drive.

C2.10.1.1 Limit use of multiple addressees and large private mailing lists. Address only those people who really need to see the message. Be judicious with "cc" addressees.

C2.10.1.2 When using public or private mailing lists, insert the mailing list into the message, and then review the names in the recipient box. Delete from the message anyone who does not really need to receive the message. Also, it is more efficient to create many small special-

purpose mailing lists than a very large one. Many times not everyone on that large list really needs to see the message.

C2.10.1.3 When replying to a message that only the sender needs to see, delete all of the other "to" and "cc" addressees from the original message. Set the default to specify "Sender Only" on replies.

C2.10.1.4 When replying to a message, delete the original attachments if they are not required.

C2.10.1.5 Use DISANet Hallways to share large documents and files with people at other DISA sites rather than attaching them to e-mail. Store the files in Hallways, then send a message to the people who need the files, telling them to retrieve them from Hallways.

C2.10.1.6 The electronic mail system has many safeguards to maintain the privacy of messages. However, conventional wisdom suggests that the user should never put anything in an e-mail message that one would be embarrassed to see in the newspaper.

C2.10.2 **E-mail Usage.** E-mail or other telecommunications systems will not be used in a way that would interfere with official duties, undermine readiness, or reflect adversely on DoD or DISA.

C2.10.3 **E-mail Prohibitions.**

C2.10.3.1 Receiving and sending authorized personal e-mail should not constitute a problem provided it serves a legitimate interest. This includes sending and receiving authorized personal e-mail that does not interfere with performance of official duties, is of reasonable duration and frequency, does not incur additional costs to DoD, and does not involve activities prohibited by other guidance. E-mail will not be used in a manner that overburdens DoD telecommunications systems.

C2.10.3.2 DISANet blocks e-mail attachments with certain extensions, such as .exe and many others. An e-mail containing a blocked attachment will have the attachment stripped, but the e-mail will be delivered.

C2.10.3.3 Do not access personal e-mail accounts, such as Hotmail, Yahoo, etc. The security features for attachments described in the previous paragraph (C2.9.3.2) are often bypassed and malicious programs may affect DISANet. Exemptions to the procedure must be approved by the IAM in writing.

C2.10.3.4 Chain letters, solicitation of business or services, sales of personal property such as trading stocks, or performing financial transactions that result in personal gain are prohibited.

C2.10.3.5 E-mail that is considered annoying or harassing to another person, such as by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language or graphics in an e-mail message is prohibited.

C2.10.3.6 Any illegal, fraudulent, or malicious activities are prohibited.

C2.10.3.7 Auto forwarding DISANet e-mail to a nonmilitary (.mil) account is prohibited.

**C2.10.4 Internet Access and Activity.** Internet or Intranet access through JITC Information systems is granted for conducting official business only. Users are permitted and encouraged to use the Internet in the gathering and sharing of information related to their tasks. Users may use government computers for incidental personal purposes such as brief communications (i.e., checking in with spouse or child, scheduling doctor appointment, brief Internet searches, etc.) so long as such use does not adversely affect the performance of official duties, is of minimal frequency and duration, does not overburden computing resources, does not result in added costs to the government, and is not for purposes that adversely reflect on this agency or the Federal government. All government regulations concerning security, privacy, propriety and use of government facilities for government business are applicable. JITC IT personnel regularly monitor customer access to the Internet services to ensure protection of networks, information, and to ensure compliance with applicable laws and regulations. Anyone using Government equipment consents to such monitoring and is advised that if such monitoring reveals possible evidence of violation of applicable laws, regulations, instructions, policies or criminal activity, designated analysts may provide the evidence to JITC management and law enforcement officials. Violation of Internet access policies may result in administrative or other disciplinary action such as actions mandated by the Uniform Code of Military Justice, performance appraisals, and personnel disciplinary actions including potential job loss. JITC policy on Internet access violations incident handling and analysis are covered in supplement 2 of this instruction.

**Prohibited uses of the Internet** include:

- Accessing sites or using software that uses excessive bandwidth such as streaming video, music stations, video/music players, viewing photographic files that are non-work related, and constantly updating stock tickers.
- Gaming, bidding at auction sites, and gambling.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography or hate literature.
- Accessing, storing, processing, displaying, or distributing partisan political, or political or religious lobbying or advocacy.
- Attempting to circumvent or defeat security or auditing systems without prior authorization.
- Sending harassing or offensive comments or jokes.
- Using another person's account or identity without his or her explicit permission.
- Permitting any unauthorized person to access a JITC or DoD-owned system.
- Storing, processing or distributing classified, proprietary, or other sensitive information on a computer or network not explicitly approved for such processing, storage or distribution.

**C2.10.5 Software on DISANet.** The only computer programs allowed on DISANet are those that have been properly tested, certified, and approved by DISANet Administration. A DISANet user may request that Network Operations install a particular computer program on the user's DISANet workstation as a local stand-alone workstation function, as long as such programs are

properly tested, certified, approved by DISANet Administration, registered in accordance with copyright laws, and do not violate government regulations with regard to security, propriety, privacy, etc. Users must ensure these programs are virus-free prior to requesting installation on their workstations. If such a program causes any of the DISA applications to fail, the stand-alone program will be removed and NOT reinstalled. Users are NOT to install executable programs (from any source) on DISANet workstations.

**C2.10.6 Temporary E-mail Accounts.** Personnel on temporary duty at the JITC fall into three categories: DISA personnel (civilian, military, or contractor) who have e-mail at their home station which is compatible with JITC e-mail; DISA personnel with incompatible home station e-mail, and non-DISA personnel.

C2.10.3.6.1 DISA personnel with compatible e-mail may be provided access to DISANet connected workstations by the host division.

C2.10.3.6.2 Other personnel who will be on duty at JITC at least 30 days may be provided a temporary account on the DISANet on a case-by-case basis. Submit a request in accordance with chapter 3.

**C2.10.7 Dial-in Access.** JITC allows dial-in access to the DISANet for official use. Users are encouraged to obtain personal firewall software for use on their personal computers (PC). This safeguard themselves, as well as DISANet assets. Network Operations can provide recommended sources or Uniform Resource Locators (URLs) for personal firewall software.

**C2.11 Automated Information Systems, Labs, and Testbeds.** Each JITC AIS, lab, and testbed has a unique mission that supports JITC's overall mission. Each represents an investment in hardware, software, personnel, data, and mission-focused knowledge. The basic protection of each system is informed personnel. System-specific briefings include security, hardware and software usage, data protection, and daily and exception operations. Each has its own security document set, including an instruction and security briefing. All personnel are required to stay informed on the requirements of their areas.

**C2.12 Use of Portable Electronic Devices Within JITC Fort Huachuca Enclave.** JITC policy on the use of portable electronic devices (PEDs), Universal Serial Bus devices, cell phones, personal digital assistants (PDA), palmtops, handheld computers, wireless devices, two-way pagers, two-way radios, audio/video/data recorders, and other small devices used to telecommunicate on the JITC enclave is defined in supplements 1 and 5.

(This page intentionally left blank.)

### C3. CHAPTER 3. JITC AIS ACCESS REQUEST

**C3.1 Form 40.** Form 40 is used to request and record Joint Interoperability Test Command (JITC) Automated Information System (AIS) access, modifications to access, and deletion of access. It is used to record all AISs, except SIPRNet access, that the user is given access to while employed at or assigned to JITC. The instructions and Form 40 are located on the drive T, in folder Word Forms as Jitc40inst.doc and Jitc40.doc.

**C3.2 DD Form 2875.** DD Form 2875, System Authorization Access Request (SAAR), is used to request and record Secret Internet Protocol Router Network (SIPRNet) Automated Information System (AIS) access, modifications to access, and deletion of access. It is used to record all JITC SIPRNet AISs access, that the user is given access to while employed at or assigned to JITC. The form is located in the DISANet Standard Application Forms.

**C3.3 JITC Information Assurance Manager (IAM) Retains Completed Forms.** When all actions have been completed (whether initial, modification, or deletion), appropriate entries will be recorded in the JITC Security32 database and the original form will be retained by the IAM.

(This page intentionally left blank.)

#### C4. CHAPTER 4. VISITORS TO JITC

C4.1 **JITC Host.** It is the responsibility of all personnel hosting visitors to the Joint Interoperability Test Command (JITC) to ensure compliance with the following Information Technology (IT) equipment procedures. IT equipment includes (but is not limited to) laptop computers and other portable electronic devices (PEDs).

C4.2 **IT Equipment.** All IT equipment brought into or removed from JITC for any use is the responsibility of the visitor's JITC point of contact (POC).

C4.3 **Visitor's Access to JITC IT Equipment.** No visitor will have access to IT equipment on any JITC system or data network without prior authorization from the applicable Information Assurance Officer (IAO). Some items for IAO consideration/action:

C4.3.1 Devices to be connected to unclassified JITC systems/networks for a period exceeding one week will be recorded on a JITC AIS Visitor Request to Connect form available on drive T, in folder Word Forms as Jitc45.doc.

C4.3.2 Devices to be connected to classified JITC systems/networks will be the subject of a JITC Visitor Request to Connect form prior to connection. This form should be completed prior to the arrival of the visitor, whenever possible.

C4.3.3 JITC is considered to be the data owner of any data obtained from or through a JITC system. Media containing such data will not be removed from JITC without the prior approval of the system IAO.

C4.3.4 Data obtained from or through a classified JITC system will be considered to be classified until reviewed by a JITC Derivative Classification Review Agent (DCRA). If determined to be classified, such media must be taken to the Security Office for review and registration.

C4.3.5 Prior to connection, the hard drive(s) of the visitor IT equipment will be scanned for malicious logic, using the latest virus scan software available from Network Operations. After the hard drive has been scanned, all diskettes associated with the visitor IT equipment will also be scanned prior to use. If a virus is detected, refer to chapter 2, paragraph 9 for appropriate actions.

C4.3.6 Personally-owned IT equipment will **NOT** be connected to JITC systems.

C4.3.7 The IAO must advise the JITC Information Assurance Manager (IAM) of any actions taken with regard to visitor accesses to JITC IT equipment.

**C4.4 Visitor's Out-Processing.** At the completion of the visit, if the visitor was processing classified, the following requirements must be strictly adhered to:

C4.4.1 The person hosting a visitor with classified IT equipment will escort the visitor to the Security Office.

C4.4.2 Classified equipment and storage media will be turned over to the Security Office for screening and disposition determination.

C4.4.3 In order to transport classified equipment or storage media, the visitor must have courier documentation from the home organization.

C4.4.4 If the visitor is not personally transporting the classified IT material, the Security Office will arrange for its transport (i.e., official USPS mailing, SECRET Internet Protocol Router Network (SIPRNet) e-mail, etc.) to the visitor's home organization IAW applicable regulations.

## C5. CHAPTER 5. JITC PERSONNEL VISITING OTHER LOCATIONS

**C5.1 Hand Receipt.** When carrying Information Technology (IT) equipment, take a copy of the hand receipt to provide proof that the equipment is lawfully in the user's possession and is a Joint Interoperability Test Command (JITC) asset.

**C5.2 Classified Material.** If a need exists to transport classified material to or from a temporary duty location, whenever possible it should be shipped by authorized means and not carried. On a case-by-case basis, authorization to hand carry may be obtained. Contact the Security Office as early as possible for authorization and assistance in making proper arrangements. Refer to DISAI 240-110-8, Information Security Program, section C, for transporting classified information.

**C5.3 Protection of IT Equipment.** When traveling with a laptop or notebook computer and other portable electronic devices (PEDs), always keep in mind that these are easily pilferable items. They can be targeted for their value as a high-dollar item as well as the value of the data they may contain. Some considerations:

**C5.3.1** Classified laptops will NEVER be left unsecured. They must be stored in an authorized General Services Administration (GSA) approved container. **DO NOT TAKE THEM TO THE HOTEL!** Have them properly stored overnight at the job site.

**C5.3.2** During travel, laptops and other PEDs must be hand carried and never checked as baggage.

**C5.3.3** Be aware of them while in such public places as airport terminals.

**C5.3.4** If possible, carry diskettes or removable hard drives separate from the laptop.

**C5.3.5** Laptops and PEDs may be stored in a locked hotel room or a locked car, but should be kept out of plain view. This may not apply to overseas travel, depending on local travel warnings. Contact the Security Office for additional information.

**C5.3.6** Laptops and PEDs will be allowed through airport screening devices. However, care must be taken to avoid theft during this process. Allow all persons in front to proceed through metal detection before placing the laptop and PEDs on the belt of the x-ray equipment. This prevents being held up by a decoy setting off the metal detector, while an accomplice removes them from the end of the x-ray belt.

**C5.3.7** Additional security countermeasures, such as cable locks, may be considered based on a risk analysis of the location to be traveled to and the sensitivity of data contained on the laptop.

**C5.3.8** Prior to travel, have the latest virus definition files loaded.

**C5.3.9** Configure the laptop with a password-protected screensaver enabled.

(This page intentionally left blank.)

**C6. CHAPTER 6. ADDITIONAL SOURCES OF IT SECURITY INFORMATION**

Users should reference the following sites as additional sources of Information Technology security information.

- <https://www.jtfgno.mil>
- <http://www.sans.org>

(This page intentionally left blank.)

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA)  
DIRECTOR'S POLICY LETTERS**

DPL 2003-7 Portable Electronic Devices (PEDs)  
DPL 2007-1 Removable Media Devices (RMDs)  
DPL 2006-12 Blackberry Devices  
DPL 2007-5 Spillages on the DISANet

(This page intentionally left blank.)

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA) POLICY ON  
PORTABLE ELECTRONIC DEVICES AND WIRELESS DEVICES**



**DEFENSE INFORMATION SYSTEMS AGENCY**

701 S. COURTHOUSE ROAD  
ARLINGTON, VIRGINIA 22204-2199

DIRECTOR'S POLICY LETTER 2003-7

1 July 2003

Portable Electronic Devices

1. **Purpose.** This Director's Policy Letter prescribes policy on portable electronic devices (PEDs).

2. **References.**

2.1 Acting DoD Chief Information Officer Memorandum, Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD), 17 May 2001.

2.2 DISAI 630-230-19, Information Systems Security Program, 9 July 1996.

3. **Background.** A portable electronic device (PED) is a generic title used to describe the myriad of small electronic items that are widely available. PEDs are used to store, process, or transmit valuable business-critical information and, if properly deployed, have the potential to increase productivity, lower communication costs, and improve the flow of information. These benefits may also pose security risks to DISA networks.

4. **Scope.** PEDs include BlackBerry devices, personal digital assistants, palmtops, handheld computers, cellular phones, two-way pagers, wireless keyboards and mice, and similar wireless devices (with or without camera or audio capabilities). PEDs do not include laptops, notebooks, and similar devices.

4.1 This policy applies to all PEDs (government, personal, or contractor-owned) that connect physically or logically to the DISA network. It also applies to all PEDs that operate in any DISA-owned or leased facilities.

4.2 This policy does not apply to PEDs in DISA Sensitive Compartmented Information Facilities (SCIFs).

## 5. Policy.

5.1 PEDs are information systems and subject to the same DISA policy and guidance governing security and use of other information systems (i.e., desktop, notebook computer, etc).

5.2 Most wireless PEDs use some form of a commercial Internet Service Provider (ISP). Use of commercial ISP service is allowed as long as sensitive unclassified information is encrypted using Federal Information Processing Standard (FIPS) 140-1 or 2, overall level 1 or 2 (Triple Data Encryption Standard or Advanced Encryption Standard) cryptography.

5.3 PEDs that synchronize with DISA networks will install DISA or DoD authorized or licensed antivirus checking software to prevent the proliferation of Trojan Horse programs and other computer viruses.

5.4 PEDs that synchronize with DISA networks will have a log-on password enabled on the device at all times. The DISA password policy will be followed for the password structure.

5.5 PEDs will have Infrared (IR) port beaming capability disabled when not in use. If the IR port cannot be disabled, it will be covered with a visor or similar object like black electrical tape.

5.6 PEDs contaminated with classified information will be turned over to the organization's Information Systems Security Officer (ISSO) or designated representative for analysis and sanitization. There will be no cost reimbursement for PEDs that cannot be sanitized.

5.7 PEDs are permitted in areas during classified processing or where confidential and above information is being discussed as long as the transmission and receive capability or functionality has been disabled or turned off. Audio, video, or photographic recording is prohibited.

5.8 PEDs will not be used to accomplish the following:

5.8.1 Process or maintain classified information.

5.8.2 Synchronize non-DISA or personal- or contractor-owned PEDs on both home computers and government computers.

5.8.3 Synchronize information across a DISA network using a wireless connection.

5.8.4 Synchronize the PED remotely by direct dial-in access to desktops without designated approving authority (DAA) approval.

5.8.5 Transmit unclassified information using Bluetooth or other wireless transmission capabilities that do not yet use FIPS 140-1/2 security mechanisms to protect information.

5.9 PEDs may be used to accomplish the following:

5.9.1 Process unclassified information from desktop workstations which includes schedules,

contact information, notes, e-mail, etc.

5.9.2 Take notes, save information, or write draft e-mails.

5.9.3 Synchronize information with desktop workstations.

5.9.4 Transmit and receive DISA e-mail using Secure/Multi-purpose Internet Mail Extension (S/MIME) enabled BlackBerry devices. Non-S/MIME two-way e-mail PED use must be approved by the DAA. The following restrictions also apply:

5.9.4.1 Users will comply with DoD public key enabling (PKE) policy (see reference 2.1).

5.9.4.2 Users will encrypt every unclassified e-mail message they transmit using cellular or ISP services.

5.9.4.3 PIN-to-PIN mode will be disabled for all devices.

5.9.4.4 Users will not remotely “hot sync” and will not generate new master keys remotely.

5.9.4.5 Users will not generate new keys from their desktops using the desktop manager. Master cryptographic keys for encrypting BlackBerry e-mail traffic should always be generated within secure U.S. Government spaces. The user will take the two-way e-mail devices to the local DISA system administrator for monthly key update.

5.9.4.6 Only DISA enterprise servers will be used to support two-way e-mail PEDs.

5.9.4.7 Two-way e-mail devices and associated desktop and server software must have the most recent software releases and service packs.

5.10 DISA-provided PEDs may be used to access unclassified network data through synchronization of PED and local desktop computers or laptops. DISA-provided PEDs are prohibited from synchronization with nongovernment workstations and laptops. PEDs will not be used to directly access the DISANet unless approved in writing by the DISA Chief Information Officer (CIO).

5.10.1 Users of DISA-provided PEDs will not download software from the Internet as specified in reference 2.2. All requests for software installation or modification on DISA-provided PEDs must be submitted through the Requirements Identification Tracking System for approval and testing. Only authorized system administrators may perform software installation.

5.10.2 Users of DISA-provided PEDs will turn in the PED prior to discharge or permanent change of assignment or office location.

5.11 If an individual has a requirement to use a PED on the DISA network, a government-owned PED must first be requested. If a government-owned PED is unavailable and mission requirements dictate the use of a PED, the DAA would approve personal- and contractor-owned PED use.

5.11.1 Personal or contractor-owned PEDs will not be connected to a DISA network without justification and DAA approval. (Mission requirements, government availability, and rationale as to how a duty position will be enhanced and why government-approved PEDs cannot meet the requirement will be included in the justification.)

5.11.2 Personal and contractor-owned PEDs should be of the same operating system as the government procures or supports. The System Security Authorization Agreement (SSAA) will include handling of PEDs and software. Personal or contractor-owned PEDs will be tracked by the ISSO and under the auspices of the local DAA.

5.11.3 Individuals must sign a PED usage statement issued by the organization property custodian agreeing to not install any additional applications or software on a PED unless they have written permission from the CIO and to update any patches or fixes or antivirus software requested by the CIO.

FOR THE DIRECTOR:

CHARLES W. STATON  
Colonel, USAF  
Chief of Staff

OPR: CIO  
DISTRIBUTION: Y

---



## DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

DIRECTOR'S POLICY LETTER 2007-1

29 Jan 2007

## Removable Media Devices (RMDs)

1. **Purpose.** This Director's Policy Letter prescribes policy on removable media devices (RMD)s.
2. **Background.** An RMD is a portable device with persistent memory that may include, but is not limited to, a laptop, removable hard disk drive, flash (thumb) drive, writable CD/DVD, floppy disk, or personal digital assistant (PDA). An RMD can be small, concealable, and easily pilferable, and significant amounts of data can be stored on it, presenting a risk for theft of government data. Additionally, malicious code can be carried on an RMD and introduced into Agency systems.
3. **Policy.**
  - 3.1 Agency systems will be configured to automatically scan any RMD for malicious code. (Malicious code includes, but is not limited to, viruses, spyware, adware, etc.)
  - 3.2 Only system administrators will possess an RMD configured to boot up workstations on the DISANet.
  - 3.3 An RMD having limited business purposes, including, but not limited to, a camcorder, MP3 or iPod-type music players, digital camera, or cell phone, must be approved by the Designated Accrediting Authority (DAA) before being connected to Agency systems.
  - 3.4 Only an RMD that is not designed to look like anything other than an RMD (e.g., an RMD designed to look like a ball-point pen) will be used on Agency systems.
  - 3.5 Any RMD containing unclassified information will be labeled with an SF 710: Unclassified (Label), prior to being placed into service.
  - 3.6 Classified information on an RMD (with the exception of classified information on a removable hard drive that is part of the standard configuration of the DISA classified network) will be encrypted using National Institute of Standards

and Technology (NIST) certified cryptography, as noted in DoDI 8500.2, Information Assurance (IA) Implementation.

3.7 Per DPL 2006-10, Protection of Personal Information (PI), the storage or transport of PI on portable media is not authorized. (Personal information (PI) is defined in DISAI 210-225-2, Privacy Program.) Exceptions are limited to storage and transport of information and applications commensurate with disaster recovery operations. Data on an RMD used for disaster recovery operations must be encrypted using NIST certified cryptography, as noted in subparagraph 3.6.

3.8 If other sensitive data, such as business sensitive data or information that is not available for public release, is stored on an RMD, the user will ensure the stored data is encrypted using NIST certified cryptography, as noted in subparagraph 3.6.

3.9 Windows Encryption File System (EFS) will be used for file and folder encryption at the user level until an enterprise encryption tool is deployed.

3.10 If there is a question about whether a portable device has persistent memory, it should be treated as if it does until it can be examined by a DISANet help desk technician.

3.11 All RMDs (personal or government-owned) are subject to search, inspection, or seizure upon entering, while on, or upon leaving any Agency facility.

3.12 Any exceptions to this policy must be authorized in writing at the directorate level and maintained by Information Management Officers (IMOs).

FOR THE DIRECTOR:

MARK S. BOWMAN  
Brigadier General, USA  
Chief of Staff

---

OPR: SPI  
DISTRIBUTION: Y



## DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

DIRECTOR'S POLICY LETTER 2006-12

22 Sep 06

## Blackberry Devices

1. **Purpose.** This Director's Policy Letter prescribes policy on Blackberry devices.
2. **Background.** A Blackberry device is a useful tool for the mobile workforce to have access to official e-mail when away from the computer or the office. Official e-mails are critical to DISA and must be protected.
3. **Policy.**
  - 3.1 All Blackberry devices will be approved by the activity Deputy Principal Director, Deputy Director, Deputy Chief, or Deputy Commander or their designee.
  - 3.2 A password will be assigned to a Blackberry device. The password must be changed by the user every 90 days. If a blackberry device is inactive for more than 15 minutes, it will be locked and can only be unlocked by the password. (The network help desk should be contacted by the user to request a password reset.)

FOR THE DIRECTOR:

MARK S. BOWMAN  
Brigadier General, USA  
Chief of Staff

---

OPR: SPI  
DISTRIBUTION: Y

(This page intentionally left blank.)



## DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

DIRECTOR'S POLICY LETTER 2007-5\*

6 Feb 2007

## Spillages on the DISANet

1. **Purpose.** This Director's Policy Letter prescribes policy on spillages on the DISANet.
2. **Background.** The DISA Information Systems Center (DISC) is responsible for sustaining the integrity, availability, and confidentiality of the information transported on the DISA Network (DISANet). This responsibility includes ensuring DISANet networks contain only information at or below the approved classification level of the network. Information introduced to the DISANet that is above the approved network classification will be termed "spillage."
3. **Policy.** As security incidents affect DISC's ability to provide services to customers because of the resources required to ensure the spillage is both contained and cleaned, the following measures will be accomplished:
  - 3.1 Actions required for sanitizing classified information from all impacted DISANet servers inside and outside the National Capital Region will be specified by the Commander, DISC, after conferring with the Chief of Staff.
  - 3.2 E-mails will be checked by DISA employees for possible classified information. If it is determined that classified information may possibly be contained in an e-mail, the procedures in paragraph 4 shall be followed.
  - 3.3 In order to offset the administrative costs associated with documenting the spillage and to bring the needed attention to these security incidents, the DISA organization that created the spillage will financially reimburse DISC \$3,000 per incident for incidents that do not require server cleanup. If the spillage requires DISANet support personnel to perform server cleanup functions, the DISA organization causing the spillage will be fined \$10,000. Of this fine, \$3,000 will be provided to DISC to cover the administrative costs of the spillage and the remaining amount will be divided among each DISANet support organization directly involved with cleaning the spill. If the spillage is of such magnitude that it requires the

impacted equipment be destroyed (degaussed), the originating organization will reimburse DISC for the equipment and the actual man-hours expended to restore the network to its normal operating configuration. Users identified as being responsible for introducing spillages may face administrative action.

4. **Procedures.** An employee who identifies or suspects a spillage has occurred will immediately notify the DISANet Control Center (DCC) at 703-607-6660 (DSN 327-6660) and the organization's Security Manager.

FOR THE DIRECTOR:

MARK S. BOWMAN  
Brigadier General, USA  
Chief of Staff

---

\*This Director's Policy letter cancels DPL 2006-4, 2 March 2006.

OPR: SPI

Distribution: Y

**JOINT INTEROPERABILITY TEST COMMAND (JITC) POLICY  
ON ANALYSIS AND INCIDENT HANDLING  
IN CASE OF INTERNET SERVICES ACCESS POLICY VIOLATIONS**

1. **Purpose.** The purpose of this document is to define JITC policy on analysis and incident handling in case of Internet services access policy violations as discussed in chapter 2 of this instruction.
2. **Applicability.** This policy applies to all military and civilian personnel assigned to or employed by JITC, contractors engaged in work on behalf of JITC, and visitors to JITC.
3. **Background.** In accordance with applicable laws and regulations JITC Information Technology (IT) personnel monitor information system use to ensure protection of networks, information, and to ensure compliance with Federal laws and regulations. All applicable employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. In addition, use of such systems is not anonymous, i.e., for each use of the Internet; the specific user ID, computer address of the system, and the locations searched is recorded. Information transmitted over an open network (such as through unsecured e-mail, the internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the Internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail messages may be re-sent to others by anyone in the chain.
4. **Analysis Methods.** JITC IT personnel (system administrators/JITC Information Assurance Manager (IAM)) employ firewalls, intrusion detection systems, and log analysis tools to detect misuse and ascertain severity of misuse. In addition, JITC expects employees to report any observed incidents of access policy violations to the JITC IAM. Upon detection or a report of access policy violation, JITC IT personnel will report incident to the JITC IAM, identify the workstation or server used by system ID and IP address, and the ID of the user logged into the network at that address. Analysis of firewall, server, and workstation logs will determine frequency and severity of the incident(s). The JITC IAM will report all incidents of access policy violations to the chief of the Business Operations Branch (JT2B).
5. **Incident Response.** JITC IT personnel will use the results of their analysis to determine whether the access policy violation was the result of accidental use (for example, inappropriate link results to a valid search engine query, or unsolicited email or pop up ads when viewing a site for information). If analysis by IT personnel indicates the access policy violation was accidental the IT personnel will review access procedures with the user. If frequency or duration of inappropriate data transfer indicates the access policy violation did not occur by accident, the JITC IAM will visit the individual's supervisor with the data and inform the supervisor the individual's access to computer resources may be denied and request the supervisor to counsel the individual accordingly. The JITC IAM will provide the Chief, JT2B with an assessment of whether the individual should be denied access to the network. If the Chief, JT2B denies access to the network, the JITC IAM will inform the supervisor the individual's access to computer resources will be denied immediately. The JITC IAM will document the incident and provide a

copy to the supervisor and the JITC Security Manager.

If the access policy violation indicates unlawful activity, the Chief, JT2B and the JITC Security Manager will notify the Commander, JITC. The JITC IAM will visit the individual's supervisor with the data and inform the supervisor the individual's access to computer resources will be denied immediately. The JITC IAM will request the supervisor to provide a time frame (within the next hour or so) by which IT personnel will secure and remove the indicated workstation.

**6. Responsibilities.** Ultimately, it is the responsibility of each employee to use government computer and network resources in accordance with this policy. The JITC IAM is responsible for reacting to and reporting incidents as appropriate. The Commander, JITC will determine the extent of any disciplinary action in the case of government violators. Disciplinary action may include performance appraisals, nonjudicial punishments, actions mandated by the Uniform Code of Military Justice, and personnel disciplinary actions.

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA) POLICY  
ON  
ACCOUNT PASSWORDS**

1. **Rules for Passwords.** DISA uses robust password security. When creating a new password, the following rules apply:

1.1. **Passwords MUST:**

- a. Contain at least **(15)** characters.
- b. Contain at least two **(2)** uppercase and two **(2)** lowercase alpha characters (A-Z, a-z).
- c. Contain at least two **(2)** numeric characters (0-9).
- d. Contain at least two **(2)** special characters (#, %, ^, &, etc.).
- e. The others may be characters of your choice.
- f. Follow all requirements from Network Operations and DISA

1.2. **Passwords MUST NOT:**

a. Contain your Username or any four (4) sequential characters from your username. For example, if your username is **cbowser**, the password cannot contain **cbow**, **bows**, **owse**, **wser**, **resw**, **eswo**, **swob**, or **wobc** in any combination of capital or lowercase letters.

b. Contain your name or any part of it. For example, if your name is **Craig Bowser**, the password cannot contain **crai**, **raig**, **giar**, **iarc**, **bows**, **owse**, **wser**, **resw**, **eswo**, or **swob**.

c. Exist in a database of common passwords. Some examples are **gibbered**, **whooping**, **overdone**, **mailbags**, **megabits**.

d. Resemble any of the last 24 passwords used by at least five characters.

e. Items are checked normally and in reverse, for example, **“password”** and **“drowssap.”**

f. Passwords must not contain dictionary words or names. This is key to a good password. **Do not** write down the password. Take the time to create a memory device for remembering your password.

g. DISANet requires you change your password every 60 days. Changing passwords across domains does not work reliably. Change your password while in your home domain.

3. **Changing Passwords.** Always use the procedure described below to change your network or Outlook e-mail password. Do not use the change password window Outlook provides or the change password option in the network logon window.

a. After logging on successfully to the DISANet, press CTRL+ALT+DELETE, holding down all three keys at once.

b. Select the “Change Password...” button.

c. Change the domain to either your logon domain, if changing the network password, or the mail domain (DISANET), if changing your Outlook password.

d. Enter both your old and new passwords.

e. Requirements for robust passwords will be enforced. Your password change will not be accepted until it meets the requirements. You will be continually re-prompted until your password meets the robust password requirements.

4. **When You Forget Your Password.** If you forget your local area network, e-mail, or calendar password, you can call the Service Desk to request a Network Operations trouble ticket to have your password reset. The Network Operations will provide you a temporary password to get you back into your application, where you will be prompted to create a new password.

## **TRANSFER OF UNCLASSIFIED DATA ON A CLASSIFIED SYSTEM TO UNCLASSIFIED MEDIA**

1. **Purpose.** This document prescribes policy and provides procedures for the transfer of unclassified data on a classified system to unclassified media.
2. **Applicability.** This document applies to all military, civilian, and contractor personnel assigned to Joint Interoperability Test Command (JITC) systems and workstations processing Secret data.
3. **Authority.** This document is published in accordance with Defense Information Systems Agency (DISA) Instruction 630-230-19, Information Systems Security Program, 9 July 1996.
4. **References.**
  - 4.1 Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS), Revision 2, 31 March 2001.
  - 4.2 Air Intelligence Agency, 690<sup>th</sup> Intelligence Support Squadron (ISS) Information Protection Flight < [https://aiaweb.lackland.af.mil/homepages/690iss/pi/toolbox/nt\\_copy2.1.0.html](https://aiaweb.lackland.af.mil/homepages/690iss/pi/toolbox/nt_copy2.1.0.html) > (CAC required).
5. **Background.** It is often necessary to copy or remove unclassified data from a classified system. This document provides the guidance necessary to safeguard classified data on the system, yet allowing unclassified data to be copied or removed.
6. **Policy.** JITC information will be protected from unauthorized disclosures, destruction, or modification while collected, processed, transmitted, stored, or disseminated.
7. **Responsibilities.**
  - 7.1 Users need to know (NTK) the vulnerabilities and risks associated with not understanding the vital importance of following the procedure, whether or not they believe the system's files contain classified data.
  - 7.2 Designated Classification Review Agents (DCRAs) assigned to validate the classification NTK the importance of their role. The Information Assurance Manager (IAM) must authorize, in writing, the DCRA to perform the validation duty and must keep the authorization on file. The IAM will not issue the authorization unless the DCRA candidate has demonstrated an understanding of the data transfer procedure.
  - 7.3 DCRAs must review all data and not assume that users or system administrators sanitized it. DCRAs must monitor the entire transfer procedure to validate the classification level.

**8. Procedures.** Only System Administrators (SAs), Information Assurance Officers (IAOs), and DCRA's are authorized to perform these procedures. The following procedures apply to the JITC environment:

**8.1 Training.** SAs and DCRA's must be trained in this procedure before proceeding. If any deviation is needed, a security officer must be notified and the deviation approved.

## **8.2 Prepare the Target Media.**

**8.2.1** If the diskette, compact disk (CD), or tape media is going to be released outside of JITC, use a new one or ensure the media is degaussed and has never been classified at a higher classification than the data to be transferred onto it.

**8.2.2** If the diskette, CD, or tape media is going to remain in JITC, you may use new or used, but ensure the media has never been classified at a higher classification than the data to be transferred, as stated in 8.2.1.

Rationale:

- New or degaussed media required when releasing outside the JITC ensures inadvertent disclosure of sensitive or classified information which recipient has no need-to-know.
- Remnant data may still exist after degaussing, so the JDCSISSS does not allow a tape to be declassified through degaussing alone (shred-then-burn and degauss-then-shred are the two accepted tape declassification procedures).

**8.2.3** Format a diskette even if it was recently formatted. Format it on an unclassified system for it to remain Unclassified. Use the following command from the Command Prompt (Disk Operating System (DOS)):

```
FORMAT A: /U
```

**NOTE:** DO NOT USE THE FILE MANAGER/WINDOWS EXPLORER TO FORMAT THE DISK. On disks formatted using the File Manager/Windows Explorer, more of the previous contents of the disk will still be readable than if the DOS "FORMAT /U" had been used" (690 ISS).

If using a tape as media, create a new folder (or new directory for a Unix system) and move the files into the newly created folder/directory.

## **8.3 Review the Data in the Parent Application Program.**

**8.3.1** The purpose of reviewing the data within the application is to see what is supposed to be visible within the application. For example, review a spreadsheet from the spreadsheet program, and review a word processing document from the word processing program. DCRA's must look for classification markings in headers and footers, and they must review all data, not just random samples.

8.3.1 The DCRA should note the size of the file on the hard drive so that the file size can be verified once the transfer is complete from the floppy disk to another hard drive.

#### 8.4 File Conversion.

8.4.1 If the document is not a text or graphic file in one of the following eight formats, convert it to one of these acceptable formats:

**TXT, RTF, HTM/HTML, JPG, BMP, PDF, GIF, FIL, NTF, NSF**

8.4.2 Copying of **DOC, PPT, XLS, MDB, TIF**, or any other type of file not listed above is prohibited.

8.4.3 Conversion Guidance:

8.4.3.1 Microsoft Word. Save the DOC file in RTF, TXT, or HTM/HTML format.

8.4.3.2 Spreadsheets and databases. Export these files as text, and then transfer the text files only.

**NOTE:** Save these files as American Standard Code for Information Interchange (ASCII) delimited files to make it easier to import them to the spreadsheet or database later.

8.4.3.3 Microsoft PowerPoint. Save the PowerPoint document as text. Transfer the text Outline/RTF or as HTM/HTML only, and reconstruct the PowerPoint on the unclassified system. If saving the presentation as HTM/HTML, save the graphics only as JPG files.

8.4.3.4 Outlook mail messages. Save the mail as TXT or HTM/HTML format. MSG format is not acceptable for human review.

8.4.3.5 Graphic files. Graphic files (JPG, BMP, and some PDF formats) cannot be saved as text, and they can only be reviewed using standard image viewers or, in the case of PDF files, Adobe Acrobat Reader. Note that there is a risk of steganography, i.e., hidden text, especially with the graphic objects. Mitigate the risk by noting the origin of the file as well as the destination of the file when transferred.

8.4.3.6 Executable files. Programmers can save the source code to transfer from the classified system and recompile it on the unclassified system. Executable programs/binary files are usually unintelligible for human review and will not be transferred.

#### 8.5 Review the Data Using a Low-Level Viewer.

8.5.1 For TXT, RTF, HTML, FIL, NTF, and NSF, use Notepad, WordPad, or any other text file viewer, to include a hex editor, that displays the entire raw contents of the file. Quit without saving the file after reviewing.

8.5.2 Review BMP and JPG files with a graphics file viewer, such as Microsoft Photo Editor.

Use Internet Explorer or Netscape to view GIF files because they can contain 3D animation and multi-page images that will not display in Photo Editor. Quit the viewer program without saving the file.

8.5.3 PDF files can be reviewed for content by using Adobe Acrobat Reader. If the PDF contains images, Acrobat is not efficient and another tool must be used (ex. MrSid).

If transferring from a Unix system, perform a “dirty word” scan on entire contents in the source directory. A perl script is one way to accomplish this task.

Use the Secure /Tar (S/Tar) utility to create and write an archive of the source directory to the media.

Example:

```
star cvf /dev/rst0 /source_directory          Create Tar file on tape
```

S/Tar must be used instead of the "tar" command. Tar pads the end of files with arbitrary data from the system and the padding data may be classified. This problem is particularly acute with files that are less than one block long (files which are more than one block long are usually padded with data from the file itself). S/Tar avoids this problem by padding files with zeros.

I. Immediately after the above operation completes, unload and write-protect the media. Then re-load the write-protected media into the drive.

II. Verify that the media contains the expected data by printing a directory of the Tar file:

```
mt -f /dev/rst0 rew                          Ensure tape is rewound (not required for floppy)
```

```
tar tvf /dev/rst0 | lpr                       Print directory of file ( | lpr may be omitted for on-
screen review)
```

III. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:

```
ls -alR /source_directory | lpr              (| lpr may be omitted for on-screen review)
```

A. Ensure that the date, time, and size information are as expected. If any unintended data was copied, the target tape should be considered classified system-high.

B. Rationale: the files which were unintentionally copied may be classified.

## 8.6 Use the Secure Copy Utility to Copy the Reviewed Data to a Diskette.

8.6.1 Before starting the Secure Copy program, make sure the formatted media prepared earlier has been WRITE-PROTECTED, and then insert the media into the drive.

8.6.2 Select the files to copy, but, before clicking on the COPY button, eject the diskette, WRITE-ENABLE the diskette, and re-insert the diskette into the drive. (This step seems tedious, but is important to note that time can be involved with marking the files for copy. As well, dependant on version, the Secure Copy utility sometimes demands a diskette in order to move the files within the interface program.)

**8.7 Use the Flush Program to Overwrite All Slack Space at the End of File(s) and All Unused Space on the Diskette.** When the Flush operation finishes, eject the floppy disk, WRITE-PROTECT it, and then re-insert into the drive. The Flush Utility program is not an intended overwrite program for declassification purposes. However, it may be used as a “clearing” program.

**8.8 Scan the Diskette.** Use the Buster program to scan the diskette for any classification markings or other keywords that may have been added to the list. The Buster program is just a text keyword search for the words listed in the text database. It will not detect unlabeled classified information, classified information in compressed files, or non-text classified information. However, it is a useful "last ditch" check to guard against mistakes.

**8.9 Remove the diskette.** Verify the write-protect, and mark it with the appropriate classification label.

**8.10 Replace the WRITE-PROTECTED Diskette in the System.** Review the data one more time to verify no additional unwanted information was copied. As a final safeguard, physically view the transferred information after running the Buster program on the disk.

**8.11 Record the Administrative Action.** Refer to table S5-1 for an example form. Keep the file for at least one year after the last entry. The form needs to specify these entries:

8.11.1 Media Verified contains no classified data.

8.11.2 Type of media used in the data transfer (diskette, CD, tape, etc.).

8.11.3 Names and signatures of the individual(s) performing the procedure and verifying the results.

8.11.4 Date and reason for the data transfer.

8.11.5 Recipient's name or the destination for the media.

**TABLE S4-1. TRANSFER OF UNCLASSIFIED DATA ON A CLASSIFIED SYSTEM TO UNCLASSIFIED MEDIA LOG**

Lab: \_\_\_\_\_

Date	File	Media	Media Destination	Recipient's Name	Verification of Data by	Verification procedure	DCRA initial	Secure Copy	Flush	Buster
<b>Reason:</b>										
Date	File	Media	Media Destination	Recipient's Name	Verification of Data by	Verification procedure	DCRA initial	Secure Copy	Flush	Buster
<b>Reason:</b>										
Date	File	Media	Media Destination	Recipient's Name	Verification of Data by	Verification procedure	DCRA initial	Secure Copy	Flush	Buster
<b>Reason:</b>										
Date	File	Media	Media Destination	Recipient's Name	Verification of Data by	Verification procedure	DCRA initial	Secure Copy	Flush	Buster
<b>Reason:</b>										
Date	File	Media	Media Destination	Recipient's Name	Verification of Data by	Verification procedure	DCRA initial	Secure Copy	Flush	Buster
<b>Reason:</b>										

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA) POLICY  
ON UNIVERSAL SERIAL BUS**

1. **Purpose.** Prescribes DISA policy on Universal Serial Bus (USB).
2. **Applicability.** This DISA policy applies to all JITC personnel and visitors.
3. **References.**
  - a. Universal Serial Bus (USB) Checklist for Sharing Peripherals Across the Network (SPAN), 6 January 2006
  - b. DISAI 630-225-7, Internet, Extranet, Intranet, and World Wide Web, 28 August 2003.
  - c. DISAI 630-230-19, Information Systems Security Program, 9 July 1996.
  - d. DISAI 270-165-2, Management of and Accountability for DISA Property, 27 August 1997.
  - e. Windows Security Technical Implementation Guides.
4. **Background.** A Universal Serial Bus (USB) is a standard developed to allow easy connection of peripheral devices to a personal computer (PC) without the requirement of complex cabling and a high level of knowledge about the configuration of the interface. The USB ports are faster and support more devices than previous PC ports. The USB ports allow a much wider range of peripherals. PEDs and jump/thumb drives may be connected and used to transmit and/or store valuable, business-critical information. If properly deployed, they have the potential to increase productivity, lower communication costs, and improve the flow of information. These benefits also pose security risks to JITC. Fire Wire Ports will follow this policy.

There are two categories of USB devices. A USB device can contain only volatile memory or no memory at all. Other devices can contain non-volatile or persistent memory.

  - a. Devices with volatile memory use the memory for temporary storage, e.g. printers, image buffers in scanners, or cache buffers.
  - b. Devices with non-volatile memory maintain the data written to them for an extended time without power being supplied, e.g. jump drives and personal digital assistants.
5. **Scope.** USB ports on the PC and USB devices are addressed in this enclosure.
6. **Use of Universal Serial Bus Policy.** In order to ensure security risks are minimized with USB ports and devices, JITC will adhere to the following restrictions:
  - a. No USB device will be attached to JITC or Government owned system without the

approval of the local IAM.

b. Only Government purchased, USB devices are to be connected to JITC or Government owned systems and PCs. (This includes Government Contractor purchased for a Government task.)

c. Privately-owned USB devices connection to JITC or Government owned systems and PCs including DISANet is prohibited.

d. The USB port function for mass storage devices will be disabled on SIPRNet machines.

e. All USB port functions will be disabled on Remote SIPRNet Workstations (RSWS).

f. Classified systems will be on case-by-case basis, but unless needed for test and/or diagnostic purposes the USB port functions will be disabled.

g. USB ports may be used on DISANet and unclassified systems.

h. Each USB device will be physically marked with the appropriate classification label.

i. Only write-protected devices will be used when moving data from USB device from unclassified to classified system.

j. Encrypt sensitive data on USB jump/thumb drives using NIST-certified cryptography. This is to protect the data from unauthorized access and disclosure if the device is misplaced or stolen.

k. All USB devices will be powered off for at least 60 seconds prior to being connected to a system.

l. The use of MP3 players, camcorders, or digital cameras will not be attached to the network without prior approval of the Designated Approving Authority (DAA).

m. Persistent memory USB devices are secured, transported, and sanitized IAW with the guidelines outlined in DoD 5200.1-R.

## **7. Other policy restrictions.**

a. Disguised USB jump/thumb drives are prohibited in the JITC enclave.

b. The system's BIOS will not be set to allow the system to boot from USB devices, except if required during system maintenance or if required for specific test requirements.