Defense Logistics Agency
INSTRUCTION

DLAI 6404
Effective April 16, 2007
Certified Current February 17, 2012

J61

Information Assurance (IA) Rules of Behavior

References: Refer to Enclosure 1.

1. PURPOSE. This Instruction delineates the responsibilities and expected behavior of all individuals (i.e., civilian, military, and contractor, referred to as the DLA workforce) that use and have access to DLA information systems. Additionally, this instruction helps foster the comprehensive knowledge of and compliance with the IA rules of behavior as a condition for continued information system access and it also sets forth requirements for verification of understanding with the rules as documented. DLA information system users must understand that they will be held accountable for their actions and are responsible for securing the data and resources in accordance with the IA rules of behavior documented herein. By adhering to the IA rules of behavior set forth in this instruction, users (e.g., General, Privileged, Secret Internet Protocol Router Network (SIPRNet)) contribute greatly to the culture of a secure, mission-oriented work environment for all DLA information system users.

2. APPLICABILITY. This Instruction applies to DLA Headquarters (HQ) and all Primary Level Field Activities (PLFA).

3. POLICY.

a. It is DLA policy that all persons requiring access to DLA information systems read, understand, and formally acknowledge through signature (digital or manual) of the applicable IA rules of behavior (e.g., General User Agreement, and if applicable, Privileged User Agreement, and/or SIPRNet User Agreement) agreement prior to being granted initial information system access or prior to a change in information system access privileges.

b. DLA information systems users are responsible for protecting DLA information systems and the information processed, stored, displayed, and transmitted. DLA information system users are also accountable for their actions when accessing any DLA network and/or application (e.g., Enterprise Business System, eWorkplace, etc.).

c. Violation of the policies associated with the IA rules of behavior at Enclosure 2 (General User Agreement, Privileged (Access) User Agreement, Secret Internet Protocol Router Network (SIPNet) User Agreement) that are incorporated as addendums to this instruction may result in disciplinary action at the discretion of an individual employee's supervisor(s) and/or senior executive management chain.

(1) DOD civilian, military, and contractor employees will potentially be subject to various levels of sanctioning (e.g., warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, removal of classification authority, termination of employment) if they knowingly, willfully, or negligently compromise or place DLA information systems and/or sensitive information at risk of compromise.

(2) Military Service members may be subject to administrative or disciplinary action as authorized by applicable regulations and the Uniform Code of Military Justice.

(3) Applicable Federal or state law(s), to include the Privacy Act, will be enforced. The Privacy Act authorizes civil and criminal penalties for violating certain provisions of the act.

4. RESPONSIBILITIES.

a. IA rules of behavior delineate the responsibilities, expectations, and individual accountability of all personnel with access to DLA information systems relative to telework, Internet usage, use of copyrighted items, unofficial use of Government equipment, the assignment and limitation of information system access privileges, handling classified (i.e., Secret and Confidential) information. The implementation of this policy and its associated rules will ensure that DLA's information systems are provided with the appropriate degree of confidentiality, integrity, non-repudiation, and availability.

b. The failure of information system users to submit a signed applicable IA Rules of Behavior agreement (i.e., General User Agreement, Privileged User Agreement, and/or SIPRNet User Agreement) to the responsible Information Assurance Officer (IAO) or Terminal Area Security Officer (TASO) can result in information system access denial, revocation of assigned information system access, and/or other administrative actions.

5. PROCEDURES.

a. A user requirement to access a DLA information system.

(1) User requires initial information system access privileges.

(2) User requires new or different access privileges.

b. IAO/TASO presents applicable IA rules of behavior agreement to the user.

(1) At a minimum, all users are required to read and formally acknowledge the General User Agreement for access to any DLA information system users.

(2) In addition to the enclosed General User Agreement, information system specific IA rules of behavior may be required for access to certain DLA information systems or for a modification of user access. Development, implementation, and governance of information system specific IA rules of behavior are the responsibility of the applicable Program/System Manager and Information Assurance Manager.

c. User reads and formally acknowledges the applicable IA rules of behavior agreement.

(1) If clarification is needed or access to specific references noted herein, the user requests assistance from the applicable IAO or TASO.

(2) The user presents the formally acknowledged (through signature) IA rules of behavior agreement to the applicable IAO or TASO.

d. DLA information system access is either allowed or denied.

(1) If signed (i.e., digitally or handwritten) verified/accepted, user receives access to or continues to access the appropriate DLA information system(s) provided other personnel actions have been approved (e.g., a favorable background investigation, etc.).

(2) If not signed verified/accepted, user is denied access.

6. EFFECTIVE DATE This Instruction is effectively immediately.

Director, DLA Strategic Plans and Policy

Enclosures(s)
Enclosure 1 – References
Enclosure 2 – IA Rules of Behavior User Agreements

ENCLOSURE 1

REFERENCES

1. DLA Instruction 6404, Information Assurance (IA) Rules of Behavior, dated April 16, 2007, superseded.
2. DLA Instruction 6401, Information Assurance (IA) Management Controls, dated December 21,2007, (currently under revision).
3. DLA Instruction 6402, Information Assurance (IA) Operational Controls, dated June 14, 2006.
4. DLA Information Operations Policy Memorandum, Digital Signature Policy, dated March 5, 2010.
5. DLA Information Operations Policy Memorandum, Removable Flash Media Usage Policy, dated May 20,2011.
6. House Resolution 2458-48, Federal Information Security Management Act of2002, January 23, 2002, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
7. Office of Management and Budget (OMB) Circular A-130, Transmittal Number 4, Appendix III, Management of Federal Information Resources, November 28,2000, http://www.whitehouse.gov/omb/circulars/al30/appendix_iii.pdf.
8. DODD 8500.01, Information Assurance, October 24,2002 (certified current as of April23, 2007), http:!/www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.
9. Department of Defense Instruction (DODI) 8500.2, Information Assurance Implementation, February 6, 2003, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.
10. DOD 5200.2-R, DOD Personnel Security Program, April 9, 1999, http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf.
11. DOD 5400.11-R, DOD Privacy Act Program, http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf.
12. DOD 5500.7-R, Joint Ethics Regulation, http://www.disa.mil/gc/pdf/directive_5500_7.pdf.
13. Chairman of the Joint Chiefs ofStafflnstruction 6510.01F, Information Assurance and Computer Network Defense, February 9, 2011, http://www.dtic.mil/cjcs directives/cdata/unlimit/6510_Ol.pdf.

ENCLOSURE 2

Defense Logistics Agency (DLA)

Information Assurance (IA): Rules of Behavior

General User Agreement

The Information Assurance (IA) rules of behavior included in this agreement delineate the responsibilities and expectations of all individuals with access to DLA information systems. All individuals will review and provide a signature (manual or digital) acknowledging these rules prior to being granted access to any DLA network and/or application.

1. What is the purpose of the lA rules of behavior?

These IA rules of behavior (including Privileged User and Secret Internet Protocol Router Network (SIPRNET) IA rules, which are contained in separate "user agreements") were established to hold users accountable for their actions and responsible for securing Government data and Information Technology (IT) resources.

2. What are lA rules of behavior?

IA rules of behavior summarize laws and requirements from various Department of Defense (DOD) and DLA policies, instructions, manuals, etc., with regard to authorized DLA information system use. IA rules of behavior establish standards of conduct that are vital to a sound and secure enterprise information operations infrastructure. The IA rules of behavior highlight the need for users to understand that taking personal responsibility for securing DLA information
and IT resources is an essential part of their mission.

3. Who is covered by these lA rules of behavior?

The IA rules of behavior apply to the DLA workforce (i.e., civilian, military, and contractor), to include authorized personnel not considered members of the DLA workforce with access to DLA information systems.

4. What are the penalties for noncompliance?

Noncompliance with these rules will result in sanctions being imposed on an individual(s) commensurate to the level of the infraction(s). Depending on the severity of the violation, sanctions may include a verbal or written/reprimand, removal of information system access for a specified period of time, reassignment to other duties or termination. Misuse of Privacy Act, sensitive (to include classified) data may result in civil and criminal charges and/or fines. Military Service members may be subject to administrative or disciplinary action as authorized by applicable regulations and the Uniform Code of Military Justice.

5. Users will:

a. Safeguard the information processed, stored, and transmitted on DLA information systems from unauthorized or inadvertent modification, disclosure, destruction, and misuse.

DLA information systems are for official use and authorized purposes in accordance with DOD 5500.7-R, Joint Ethics Regulation, section 2-301.

b. Comply with safeguards, policies, and procedures to prevent unauthorized access to DLA information systems.

c. Comply with terms of software licenses and only use DLA licensed and authorized software. Additionally, users will not install single license software on shared hard drives (or servers) without prior approval.

d. Complete periodic IA awareness training when made available.

e. Use DLA Internet access and electronic mail (email) services for non-official purposes only under the following circumstances: I) Usage does not adversely affect the employee's performance or accomplishment of the DLA or DOD mission and usage does not reflect adversely on DLA, DOD, or the Federal Government as a whole; 2) Usage will occur on breaks, lunch periods, and non-duty hours; and 3) Usage precludes any unnecessary costs or appearance of impropriety to the Federal Government.

f. Not transmit sensitive information over the Internet unless it has been encrypted and digitally signed using a Common Access Card (CAC) based DOD public key certificate.

g. Digitally sign email containing attachments and embedded hyperlinks.

6. Not use DLA Internet access and email services to:

a. Knowingly view, receive, or transmit material with pornographic content.

b. Conduct illegal activities and soliciting for personal gain.

c. Download copyrighted software without express permission.

d. Download without ensuring protection against viruses.

e. Misrepresent personal opinion as official information.

f. Knowingly distribute chain letters, extremist or terrorist material advocating the violent overthrow of the government and/or material or jokes that demean or ridicule others on the basis of race, creed, religion, color, sex, disability, or national origin.

g. Not engage in deliberate activities that overload network resources (e.g., downloading music or video files). Network bandwidth consumption caused by such downloads may inhibit or prohibit network service to other users.

h. Promote partisan political activity.

i. Access, store, process, display, distribute, transmit, or view material that is abusive, harassing, defamatory, vulgar, profane; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, Federal, national, or international law.

j. Access, store, process, or distribute Classified, Proprietary, or Privacy Act protected information in violation of established security and information release policies.

k. Use the DLA network resources for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay). This does not prohibit the use of a local intranet for bulletin boards/want ads.

l. Disseminate religious information umelated to DLA's established religious program;

m. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers, charitable fund raisers).

n. Gamble, wager, or place any bets.

NOTE: Although DLA uses Web filtering technology to prevent access to inappropriate Web sites, it is not a complete solution and the ability to access a Web site does not mean that it is not prohibited. It is a user's responsibility to recognize the accountability assigned when given authorized access to any DLA information system. Individual user activity is recorded, including Internet and Intranet sites and files accessed.

o. Not knowingly write, code, compile, store, transmit, or transfer unauthorized software code, Trojan horse programs, or malicious software code, to include viruses, logic bombs, worms, and macro viruses into any DLA information system.

p. Not attempt to bypass the Web filtering system (e.g., installing proxy bypass software).

q. Not share account passwords with anyone, including Personal Identification Numbers (PIN) for CAC associated with the Public Key Infrastructure.

r. Not attach any non-DLA issued device (e.g., personally owned Personal Digital Assistants, wireless devices) to any DLA information system without prior approval.

s. Not utilize any removable storage media (e.g., thumb drives, memory sticks, floppy disks, camera flash memory cards, high capacity ZIP floppy drives, secure digital cards other than compact discs (CD) or DVDs without prior approval.

t. Encrypt all data not approved for public release copied to a CD or DVD using approved software. Contact your local Information Assurance Officer (lAO) or help desk for assistance.

u. Immediately report known or suspected incidents to the responsible Information Assurance Manager in accordance with the DLA Computer Incident Response Guide.

v. Log out prior to leaving his/her desk/office/cubicle/work area at the end of his/her work day.

w. Lock his/her workstation when unattended for an extended period of time.

x. Remove his/her CAC from workstation when unattended.

y. Not attempt to modify automated screen-lock functions performed by the information system.

z. Scan files received from untrusted sources prior to opening them. For assistance with this function, please contact your local lAO or help desk.

aa. If applicable, process classified data on classified information systems only.

ab. Not use shared drives to relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those authorized to access the data.

ac. Be cognizant of all applicable DLA IA polices.

7. Consent to Monitoring Provision

a. In addition to formally acknowledging through signature, the required provisions documented above, all users with access to a DOD information system are required to read and acknowledge the following consent to monitoring provision.

b. By signing this document, you acknowledge and consent that when you access DOD information systems:

c. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

d. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Note: Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and

their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(5) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(6) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(7) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(8) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

(9) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(10) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(11) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (law enforcement for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise- authorized use or disclosure of such information.

(12) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a

banner is used, the banner functions to remind the user of the provisions that are set forth in this user agreement, regardless of whether the banner describes these provisions in full detail or provides a summary of such conditions. In addition, this applies regardless of whether the banner expressly references this user agreement.

I acknowledge receipt of this General User Agreement, understand my responsibilities, and will comply with these provisions when accessing a DLA information system.

Print Name

Date

Signature

DLA Organization/Activity

Defense Logistice Agency (DLA)

Information Assurance (IA): Rules of Behavior

Privileged (Access) User Agreement

Privileged users are authorized users who have the ability to modify secure configurations (e.g., access controls, etc.) or bypass IA controls enforced by DLA information systems (e.g., account setup, account termination, account resetting, auditing).

1. What is the purpose of the lA rules of behavior?

These IA rules of behavior (including general user and Secret Internet Protocol Router Network (SIPRNet) IA rules, which are contained in separate "user agreements") were established to hold users accountable for their actions and responsible for securing Government data and Information Technology (IT) resources.

2. What are lA rules of behavior?

IA rules of behavior summarize laws and requirements from various Department of Defense (DOD) and DLA policies, instructions, manuals, etc., with regard to authorized DLA information system use. IA rules of behavior establish standards of conduct that are vital to a sound and secure enterprise information operations infrastructure. The IA rules of behavior highlight the need for users to understand that taking personal responsibility for securing DLA information
and IT resources is an essential part of their mission.

3. Who is covered by these lA rules of behavior?

These IA rules of behavior apply to the DLA workforce (i.e., civilian, military, and contractor), to include authorized personnel not considered members of the DLA workforce with access to DLA information systems. In particular, Privileged Users include, but are not limited to, System and Network Administrators, Web and Database Administrators, Firewall and Application Administrators, Software Developers, and Security Administrators (e.g., IA Managers (IAM), IA Officers (IAO)).

4. What are the penalties for noncompliance?

Noncompliance with these rules will result in sanctions being imposed on an individual(s) commensurate to the level of the infraction(s). Depending on the severity of the violation, sanctions may include a verbal or written/reprimand, removal of information system access for a specified period of time, reassignment to other duties or termination. Misuse of Privacy Act, sensitive (to include classified) data may result in civil and criminal charges and/or fines. Military Service members may be subject to administrative or disciplinary action as authorized by applicable regulations and the Uniform Code of Military Justice.

NOTE: The rules of behavior delineated in the DLA "General User" agreement are applicable to all DLA information system users and used in conjunction with the privileged user rules of behavior documented herein.

5. Privileged Users will:

a. At a minimum, have undergone an appropriate personnel security investigation commensurate with the IT level (e.g., IT- I [privileged], IT- II [limited privileged]) required to perform the duties assigned.

b. Hold a U.S. Government security clearance, when privileged access is required for an information system storing, processing, and/or transmitting classified (i.e., Secret) information.

c. Configure and operate information systems and IA controls in accordance with applicable Security Technical Implementation Guides (STIG) and DLA policies and procedures.

d. Notify the responsible lAO of any configuration changes that might adversely impact the information system.

e. If applicable, create user accounts only after receipt of an approved system access authorization request (automated or manual).

f. Establish and manage authorized user and system (e.g., service accounts) accounts for DLA information systems, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

g. Not add/remove any users' names to the Root Level, Domain Administrators, Local Administrator, or Power Users group without the prior approval of the system manager and/or lAM.

h. Access only that data, control information, software, hardware, and firmware for which you are authorized access to and have a need-to-know.

i. Not access sensitive application data for other than official purposes based on roles and responsibilities associated with mission requirements.

j. Maintain separate accounts for administrative transactions (privileged account) and for day-to-day user transactions (general user account). This includes the use of privileged accounts only for privileged functions and the use of your general user account for all non-privileged functions (e.g., email, Web browsing, etc.).

k. Comply with the privileged account password construct requirement, if applicable.

l. Not share access to privileged accounts (e.g., will not share alternate tokens/personal identification numbers (PIN) or privileged account password(s) with unauthorized personnel).

m. Assume only those roles and privileges for which you are authorized.

n. Not install, modify, or remove any hardware or software (i.e., freeware/shareware and !A-related tools) without written permission/approval from the system manager and/or lAM.

o. Not obtain, install, copy, transfer, or use software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

p. Not knowingly write code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.

q. Limit the use of vulnerability scanning tools for their intended purposes and only after proper coordination with and approval by the responsible system manager and/or IAM.

r. Not attempt to run "sniffer" or hacker-related tools on any information system unless authorized by the Designated Approving Authority and system manager/lAM. This includes the introduction of any foreign devices (non-approved equipment) to any DLA information system without specific authorization.

s. Immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate system manager and/or IAM.

6. Consent to Monitoring Provision

a. In addition to formally acknowledging through signature, the required provisions documented above, all users with access to a DOD information system are required to read and acknowledge the following consent to monitoring provision.

b. By signing this document, you acknowledge and consent that when you access DOD information systems:

c. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

d. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Note: Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or

monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(5) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(6) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(7) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(8) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

(9) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(10) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(11) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (law enforcement for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise- authorized use or disclosure of such information.

(12) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions reminds the user of the provisions that are set forth in this user agreement, regardless of whether the banner describes these provisions in full detail or provides a summary of such conditions. In addition, this applies regardless of whether the banner expressly references this user agreement.

I acknowledge receipt of this Privileged User Agreement, understand my responsibilities, and will comply with these provisions when accessing a DLA information system.

Print Name	Date
Signature	DLA Organization/Activity

Defense Logistics Agency (DLA)

Information Assurance (IA): Rules of Behavior

Secret Internet Protocol Router Network (SIPRNet) User Agreement

DLA SIPRNet users consist of individuals with the appropriate security clearance and a valid need-to-know. Authorized SIPRNet users will have limited access to a secure host providing classified (Secret) electronic mail (email) services, directory services, shared file and print services, communications services, data-backnp services, and limited access to classified Web sites and Web-based services available on the SIPRNet.

NOTE: The rules of behavior delineated in the DLA "General User" agreement are applicable to all DLA information system users and used in conjunction with the SIPRNet user rules of behavior documented herein.

1. SIPRNet Users will:

a. Complete the DLA Classified Basic Course prior to accessing the SIPRNet. Contact your responsible Information Assurance Officer (lAO) and/or Terminal Area Security Officer (TASO) for access to this training course.

b. If applicable, change his/her initial SIPRNet passwords upon initial login and will not release their new password to anyone.

c. Not share account passwords or personal identification numbers (PIN). SIPRNet Passwords and PINs must be protected at a level commensurate with the sensitivity level or classification level of the information to which they allow.

d. Report any compromise or suspected compromise of classified information to include passwords, PINs, or safe combinations to the responsible Information Assurance Manager (lAM).

e. Immediately report any security incidents and potential threats and vulnerabilities involving SIPRNet resources in accordance with the DLA Classified Information Spillage Instruction and Department of Defense Regulation 5200.1-R.

f. Take appropriate actions to prevent unauthorized viewing and disclosure of classified information.

g. Not disclose classified data prior to verification that individual has the appropriate security clearance (e.g., Secret or Top Secret) and a valid need-to-know.

h. Secure all classified property (e.g., documentation, removable hard drives) in an approved General Services Administration (GSA) safe when unattended, not in use, and at the end of the duty day.

i. Not attempt to utilize removable storage/flash media (e.g., DVDs, CDs, thumb drives, camera flash memory cards, etc.) with prior approval/authorization.

(1) Writeable CDs and DVDs are only authorized on the SIPRNet to perform data transfers from unclassified sources to SIPRNet, and only if approved by the DLA Designated Approval Authority (DAA). You should contact your IAO/IAM if you need to transfer data from unclassified sources to the SIPRNet and the data transfer has not already been approved by the DLADAA.

(2) Only personnel authorized by the local J6 Site Director are authorized to perform data transfers from unclassified data sources to SIPRNet in accordance with specified guidance.

(3) The use of removable flash media will be facilitated in accordance with the DLA Removable Flash Media Usage Policy Memorandum or associated DLA instruction in which this policy memorandum may be incorporated.

j. Not take wireless devices (e.g., cell phones, pagers, personal digital assistants (PDA)) into an area where classified information is being discussed or processed without written approval from the DLA DAA.

k. Not remove equipment or removable hard drives from the work area without appropriate written approval from the responsible IAM and/or authorized SIPRNet point of contact.

l. Only reproduce classified information on approved copy machines and/or printers and apply the appropriate classification markings.

m. Dispose of classified waste appropriately in accordance with DLA policy and procedures.

n. Not attempt to circumvent IA Technical, Management, and Operational controls (e.g., downloading classified data on removable storage media without prior approval).

2. Consent to Monitoring Provision

a. In addition to formally acknowledging through signature, the required provisions documented above, all users with access to a DOD information system are required to read and acknowledge the following consent to monitoring provision.

b. By signing this document, you acknowledge and consent that when you access DOD information systems:

c. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

d. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Note: Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to
personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(5) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(6) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(7) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal

legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(8) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

(9) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(10) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(11) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (law enforcement for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise- authorized use or disclosure of such information.

(12) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions remind the user of the provisions that are set forth in this user agreement, regardless of whether the banner describes these provisions in full detail or provides a summary of such conditions. In addition, this applies regardless of whether the banner expressly references this user agreement.

I acknowledge receipt of this SIPRNet User Agreement, understand my responsibilities, and will comply with these provisions when accessing a DLA information system.

Print Name	Date
Signature	DLA Organization/Activity