

Defense Logistics Agency (DLA)
Information Assurance (IA)

1. REFERENCES

- 1.1. DLAR 5200.17, Security Requirements for Automated Information and Telecommunications Systems, dated June 9, 1993.
- 1.2. Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510, DoD Global Information Grid (GIG) Information Assurance, dated June 16, 2000.
- 1.3. DLA Information Technology Solutions, Version 1.0, dated April 2000.
- 1.4. Deputy Secretary of Defense Memorandum Serial U07287/99, Department of Defense Public Key Infrastructure, dated August 12, 2000.
- 1.5. Deputy Secretary of Defense Memorandum Serial U17006/99, Smart Card Adoption and Implementation, dated November 10, 1999.
- 1.6. DoD 5200.2-R, Personnel Security Program, dated January 1997.
- 1.7. Chairman Joint Chiefs of Staff Instruction 6510.01C, Information Assurance and Computer Network Defense, dated May 1, 2001.
- 1.8. through 1.28., see Enclosure 1.

2. PURPOSE

- 2.1. This directive:
 - 2.1.1. Establishes DLA IA policy, defines IA roles and assigns responsibilities, and provides guidance to ensure the protection of information necessary to the execution of the DLA mission.
 - 2.1.2. Cancels reference 1.1.
 - 2.1.3. Supplements reference 1.2.

3. APPLICABILITY AND SCOPE:

- 3.1. The concept of Defense-In-Depth is DoD's response to threats to the GIG. IA is the implementation of Defense-In-Depth. This guidance and policy applies to:

- 3.1.1. All assigned civilian, military, and contractor personnel at DLA Headquarters staff elements, joint program offices, and all DLA Field Activities (to include commercially-operated facilities). Herein referred to, in context, as "DLA" or "DLA employee."
- 3.1.2. All DLA-owned or controlled electronic contemporary, legacy, and emerging information systems and technologies, to include those under contract to DLA, that receive, process, store, display, or transmit DLA information, regardless of classification, mission category, or sensitivity. Included are portable electronic devices in either or both wired and wireless modes.
- 3.1.3. All Information Technology (IT) acquisitions, statements of work, requests for proposals, Memoranda of Understanding/Memoranda of Agreement (MOU/MOA), and similar documents for the acquisition and operation of IA equipment, software, maintenance, or other professional services which contain statements that apply to this directive.
- 3.1.4. All implementing instructions, plans, and handbooks for this directive covering IA topics including certification and accreditation (C&A), enclave boundary defense, information system security management and control, access control, public key infrastructure, passwords, emergency response, networks and web sites, security, awareness, training, and related IA issues.

4. POLICY:

- 4.1. DLA shall comply with DoD IA policy as defined in the references.
- 4.2. All DLA information systems and enclaves shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation and availability services that reflect a balance among the value of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; and cost effectiveness.
- 4.3. DLA shall follow the principle of risk management. Risks shall be prioritized and necessary protection requirements determined, including cost-effective technical, procedural, and physical safeguards commensurate with the risk to the mission of the organization.
- 4.4. As part of the GIG, DLA IA efforts shall follow the DoD IA Technical Framework (IATF). DLA shall update and maintain reference 1.3 and implement the strategy of Defense-in-Depth. Computer Network Defense (CND) policies and procedures shall be used in support of overall DoD-wide network integrity.
- 4.5. DLA shall participate in the DoD CERT Reporting Program in accordance with reference 1.2.

- 4.6. Managed by the DLA Computer Emergency Response Team (CERT), an Agency-wide audit capability shall be established to ensure the DLA IT infrastructure is identified and protected.
- 4.7. Data files containing DLA IA metrics and control information, or other data which is considered sensitive when aggregated, are to be considered "For Official Use Only (FOUO)" (or higher based on the classification of the data) and encrypted when transmitted.
- 4.8. Classified information will be appropriately encrypted (using approved encryption devices) and protected when transmitted electronically.
- 4.9. The use of digital certificates or tokens for DLA information systems shall be implemented in accordance with the DoD PKI policy and references 1.4 and 1.5.
- 4.10. Exchange of unclassified information between DoD and its vendors and contractors requiring IA services will use validated DoD PKI certificates obtained from approved External Certificate Authorities (ECAs).
- 4.11. Access to DLA systems, networks, and web sites shall be granted on a need-to-know basis and in accordance with reference 1.6. for clearance, special access, and Automated Data Processing (ADP) IT category designation requirements and qualifications. Privilege-based access controls shall follow the principle of "least privilege," disallowing all access privileges that are not explicitly permitted.
- 4.12. Foreign nationals may be permitted access to the Non-classified Internet Protocol Router Network (NIPRNet) following recommendation by the local Designated Approving Authority (DAA) and approval of the Agency Director. All foreign national requests for access must comply with the host Military Department investigative requirements and the provisions of reference 1.6.
- 4.13. All contractor and foreign national users requiring access to dot (.) mil e-mail shall be identified in accordance with reference 1.7.
- 4.14. DLA systems requiring logon authentication shall, as a minimum requirement, use a properly administered and protected password consisting of at least eight characters to include a mix of at least one of each of (a) uppercase letters, (b) lowercase letters, (c) numbers, and (d) special characters.
- 4.15. Passwords for access to DLA systems, networks, and web sites shall not be shared or exchanged between or among users.
- 4.16. All individuals attempting access to DLA information systems shall be notified of the rules of behavior concerning the use of the systems.

- 4.17. IT solutions shall be implemented to isolate non-DLA information systems that have access to and from the Internet and DLA systems. The isolation solution shall be either physical or technical, such as an approved boundary protection product, and be in accordance with applicable policies for firewalls, intrusion detection, and web site administration.
- 4.18. Safeguards shall be in place to ensure proper access to a DLA system, network, or web site at a level commensurate with an individual's assigned functions and the access modified as assigned functions change. Each DLA employee shall be advised of their responsibilities associated with their use of the system and of their being held accountable for their actions relative to maintaining a secure system.
- 4.19. Safeguards shall be in place and maintained to provide secure remote dial-in capabilities.
- 4.20. Each DLA system, network, and web site C&A shall be documented by means of a System Security Authorization Agreement (SSAA) in accordance with references 1.8 and 1.9.
- 4.21. Following receipt of the Approval To Operate (ATO), the SSAA shall be updated and approved by the DAA within 3 months of any modification which affects the security architecture or risk to system/application. Revalidation shall occur annually. Use of the system shall be reaccredited at least every 3 years or when a change is made that alters the security or integrity of the existing configuration.
- 4.22. The DLA Comprehensive Information Assurance Knowledgebase (CIAK) shall be a secure, password-protected database and used by all DLA activities to store, update, and otherwise maintain their data related to DLA information systems, networks, and web sites.
- 4.23. All inter-connections of DLA information systems, both internal and external, shall be managed to continuously minimize community risk. Connection to the Defense Information Systems Network (DISN) NIPRNet will follow the Defense Information Systems Agency (DISA) connection approval process. Request for waivers shall be forwarded to DLA Field IT Services (J-632) for approval and to DLA IA (J-633) for information purposes.
- 4.24. All DLA systems, networks, and web sites processing classified information shall be certified and accredited in accordance with references 1.8 and 1.9 prior to actual commencement of processing.
- 4.25. The use of mobile code in DLA systems, networks, or web sites shall be controlled in accordance with reference 1.10, and shall be registered with J-6 as part of an SSAA.
- 4.26. All biometrics technology intended for integration into DLA information systems shall be coordinated with the DoD

Biometrics Management Office and acquired in accordance with established DoD policy and procedures.

- 4.27. All DLA System Change Requests (SCRs) and Configuration Control Board (CCB) agenda items shall be formally reviewed by the CCB for IA impact. For those that demonstrate an impact, a mitigation strategy shall be developed and implemented as part of the SCR or agenda item. Review and analysis of the proposed mitigation strategy shall be provided to DLA IA (J-633) and the DLA CERT.
- 4.28. Public domain software products (i.e., freeware) may be used in DLA information systems if an official requirement is established, the product is assessed for IA impacts, and both the requirement and the product are approved by the responsible DAA.
- 4.29. All IA-related, government off-the-shelf and Commercial Off-the-Shelf (COTS) hardware, firmware, and software components and IT products shall be evaluated and acquired in accordance with reference 1.11 and other applicable national and DoD policy and guidance.
- 4.30. IA program reviews shall be conducted periodically to comply with the regulatory guidance that defines the effectiveness and adequacy of the safeguards for operationally accredited systems, networks, and web sites. Systems shall be subject to active penetration and other forms of testing.
- 4.31. Personally owned Personal Electronic Devices (examples are listed in enclosure (2), number 40) are not authorized to connect/synchronize to the DLA network unless specifically approved in accordance with this directive.
- 4.32. In that wireless technology (e.g., infrared, acoustic, radio frequency) stores, processes and/or transmits information outside the physical confines of DLA-controlled areas and introduces additional vulnerabilities, they shall not be connected to DLA systems without the approval of the DAA. In addition:
 - 4.32.1. Unclassified information will be encrypted to and from the wireless device; PKI (references 1.4 and 1.5) is required for access to DLA systems; and the minimum requirements of references 1.8 and 1.9 are applied.
 - 4.32.2. Classified information shall be protected to the same degree and in the same manner as is applied to the highest classification at which that system utilized is certified to process. (reference 1.12.)
- 4.33. All purchased and/or licensed software shall be used in accordance with the vendor's established copyright/license provisions. All DLA software shall be developed, managed, and stored in a manner to minimize the risk of errors, bugs, and/or malicious code.

4.34. The DLA IA Awareness, Training, and Education Program shall be implemented and managed as part of the Defense-in-Depth strategy and shall comply with references 1.13 through 1.17.

4.34.1. Initial orientation and annual end user refresher training in computer security awareness and accepted computer security practices is required for all DLA employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of the Agency.

4.34.2. IT professionals shall be trained to attain and maintain the required levels of expertise commensurate with the specific IA duties assigned.

4.35. Classified information processed by DLA networks and systems must be protected in accordance with reference 1.18.

4.36. If the provisions of this directive cannot be achieved as required, requests for a waiver or time extension may be submitted. These requests should be submitted to the Director, Information Operations/Chief Information Officer (CIO) (J-6) via the Chief, IA Division (J-633), with sufficient justification and signed by the DAA.

5. RESPONSIBILITIES:

5.1. The Director of DLA shall:

5.1.1. Develop and implement an IA Program consistent with the Clinger-Cohen Act (reference 1.15) and the Defense IA Program (DIAP).

5.1.2. Establish the appropriate INFOCON (Alpha, Bravo, Charlie, or Delta) when DLA Headquarters or any field site comes under a cyber attack that impacts the ability to provide uninterrupted support to the warfighter.

5.1.3. By means of this directive, appoint DAAs for all DLA information systems for which they have responsibility.

5.1.4. Comply with established accreditation and connection approval processes required for all DoD information systems.

5.2. The DLA Director of Information Operations (J-6)/CIO shall:

5.2.1. Direct, administer, and provide oversight to the DLA IA Program, under the authority of reference 1.15.

5.2.2. Serve as the DAA for all DLA mission critical and mission support systems, networks, and web sites.

5.2.3. Assign J-6 representative to the DLA INFOCON Advisory Committee as a voting member and provide the DLA Director

recommendations to support the issuance of an INFOCON action, when required.

- 5.2.4. Appoint headquarters PKI Registration Authorities (RA) and Local Registration Authorities (LRA), as required, for PKI.
- 5.2.5. When required, ensure DLA-owned or operated information systems are enabled to use biometrics for positive access control in accordance with published DoD policy and procedures.
- 5.2.6. Coordinate all IA research and technology initiatives under their purview with the Director, Defense Research and Engineering (DDR&E).
- 5.2.7. Plan, budget, and execute adequate resources in support of IA.
- 5.2.8. As information owner:
 - 5.2.8.1. Establish information classification, sensitivity, and need-to-know for DLA component-specific information.
 - 5.2.8.2. Establish information owner designees for all DoD component-specific information systems.
 - 5.2.8.3. Assign mission categories to DLA component-specific information, systems, and enclaves.

5.3. The Staff Director, Technology Services and Infrastructure Support, (J-63) shall:

- 5.3.1. Serve as the DLA Certification Authority (CA) for DLA mission critical and mission support systems, networks, and web sites.
- 5.3.2. Provide policy guidance and responsibility for the Agency level operational protection, detection, and response capability in the form of a DLA CERT. This capability incorporates the DLA INFOCON, IA Vulnerability Management (IAVM) program, incident reporting, vulnerability assessment, and red team processes.
- 5.3.3. Through the National IA Program (NIAP) and in accordance with NSTISSP No. 11 (reference 1.11), establish criteria and processes for evaluating and validating all IA related COTS products used to provide assurance services for DLA information systems.
- 5.3.4. Validate or define system performance, availability, and functionality requirements as normally specified in the Operational Requirements Document (ORD).

- 5.3.5. Provide for enterprise-wide specification, acquisition, provisioning, and configuration of IA technologies, including but not limited to firewalls and intrusion detection systems.
 - 5.3.6. Ensure the DLA General Counsel approved notice of privacy rights and security responsibilities are provided in a banner to all DLA individuals attempting initial access to DLA information systems.
 - 5.3.7. Verify the ability to comply with the SSAA during continuity of operations.
 - 5.3.8. Ensure development of integrated and consistent Continuity of Operations Plans (COOP) for all mission essential systems, networks, and web sites and assure their periodic testing.
 - 5.3.9. Ensure compliance with established DISA connection approval processes for all information systems connections.
- 5.4. The Chief, IA Division (J-633) shall:
- 5.4.1. Assign a CA representative for all DLA systems, networks, and web sites.
 - 5.4.2. Participate as a voting member of the DLA INFOCON Advisory Committee.
 - 5.4.3. Oversee development and operation of Metrics and Controls for Defense-in-Depth.
 - 5.4.4. Collect and report IA management financial and readiness data to meet DoD IA internal and external reporting requirements.
 - 5.4.5. Establish and maintain projects in, and assign project leaders to, at a minimum, the areas of awareness, training, and education; enclave boundary defense (firewalls, virtual private networks (VPNs), and intrusion detection systems); access controls (Passwords and Logon Identification); alert taskings; vulnerability assessments; incident response and INFOCON; C&A; and IA Architecture. These project areas may be adjusted as the DLA IA Program matures.
 - 5.4.6. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.
 - 5.4.7. Establish DLA CND services to coordinate and direct Agency-wide CND and CND reporting with direct involvement of the DLA CERT.

- 5.4.8. Provide Agency-wide guidance regarding the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) C&A process for the DLA enterprise.
 - 5.4.9. Promote sharing of emerging technologies relating to IA.
 - 5.4.10. Ensure that IA requirements are addressed and visible in DoD component IT-dependent and IT-related investment portfolios and programs.
 - 5.4.11. Ensure that IA awareness, training, education, and professionalization programs are provided to all DLA military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DLA information systems.
- 5.5. The Staff Director, Command Security Office (DSS-S) shall:
- 5.5.1. Provide intelligence support to the DLA INFOCON advisory committee chairperson.
 - 5.5.2. Participate as a voting member of the DLA INFOCON advisory committee.
- 5.6. The Chief, Contingency Plans and Operations Division (J-341) shall:
- 5.6.1. In coordination with J-633, activate the DLA INFOCON Advisory Committee upon receipt of a USSPACECOM INFOCON Change Notice, or when DSS-S, DLA CERT, or Joint Task Force-Computer Network Operations (JTF CNO) initiates a warning that requires the DLA Director to establish an INFOCON action.
 - 5.6.2. At the request of J-633, take the required J-3 staffing actions to provide input to J-6, and the DLA Director when applicable, with recommendations to support the issuance of an INFOCON change.
 - 5.6.3. Prior to release by J-6, obtain J-3 coordination on the INFOCON activation messages released to Agency activities for appropriate action.
- 5.7. DLA CERT shall:
- 5.7.1. Conduct system scans and use related methodologies to facilitate defensive actions to monitor, assess, and respond to system, network, and web site vulnerabilities.
 - 5.7.2. Establish a computer incident response capability to:
 - 5.7.2.1. Monitor and detect suspicious, unauthorized, or malicious activity;

- 5.7.2.2. Receive and relay warnings of threats from DLA organizations and from the DoD CERT;
- 5.7.2.3. Report computer security incidents to DLA Headquarters IA (J-633), DLA Criminal Investigations Activity (DI), and DoD CERT, as appropriate.
- 5.7.3. Coordinate IA protective measures and implement DoD-wide CND direction from U S Commander in Chief Space Command (USCINCSpace) for DLA networks.
- 5.7.4. Coordinate all JTF-CNO and DoD CERT directives, taskings, alerts, and advisories.
- 5.7.5. Recommend appropriate steps for DLA activities to take in response to computer and network security incidents, and if unable to obtain satisfactory field activity action within a reasonable time period, take such action as may be necessary to protect DLA systems, and other DoD information assets. Such action may include, but is not limited to, blocking specific network traffic, disabling specific network services, and disconnecting systems and networks.
- 5.7.6. Conduct IT hardware and software audits to identify assets and ensure DLA IA security requirements have been properly implemented.
- 5.7.7. Conduct periodic onsite reviews of field activity IA operations and programs.
- 5.7.8. Participate as a member of the DLA INFOCON Advisory Committee.
- 5.8. Headquarters Directors and Commanders/Directors/Administrators of DLA Field Activities shall:
 - 5.8.1. Ensure compliance with this policy directive.
 - 5.8.2. Plan, budget, and execute a plan to apply sufficient resources to achieve an acceptable level of security and to remedy security deficiencies in support of the IA Program.
 - 5.8.3. Approve and promulgate procedures to implement DLA IA policies within their departments or staff offices.
 - 5.8.4. Ensure that IA requirements, to include security audits and C&A, are included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD information systems and supporting infrastructures.
 - 5.8.5. Serve as DAA for unique or site-specific systems, networks, web sites, and applications under their program direction.

- 5.8.6. Ensure each mission critical, mission support, and administrative system within the activity has a System Administrator (SA), designated in writing, to ensure compliance with DoD and DLA IA regulations and guidelines.
- 5.8.7. Ensure appropriate and sufficient number of security staff ISSMs/Information System Security Officer(s)(ISSO(s))/ Terminal Area Security Officers (TASOs) are appointed in writing to implement the provisions of this directive and supporting guidance at each system or site, and to follow direction provided by the DLA CERT.
- 5.8.8. Ensure adequate resources are provided to interact and coordinate with the DLA CERT for CND.
- 5.8.9. Provide site access and support for IT audits to ensure DLA IA security requirements have been properly implemented.
- 5.8.10. Ensure that IA awareness, training, education, and professionalization programs are provided to all DLA military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DLA information systems.
- 5.8.11. Ensure DLA General Counsel approved notice of privacy rights and security responsibilities are provided in a banner to all DLA individuals attempting initial access to DLA information systems.
- 5.8.12. Ensure that all personnel under their purview receive security awareness training on an annual basis.
- 5.8.13. Ensure that only Communications Security (COMSEC) equipment acquired through the National Security Agency (NSA) as the centralized COMSEC acquisition authority, or through NSA designated agents, are used to protect classified systems.
- 5.8.14. Appoint RAs and LRAs.
- 5.8.15. Ensure that the IT Chief initiates INFOCON actions when directed by DLA CERT.
- 5.8.16. Support DLA CERT system scans and related vulnerability assessment techniques.
- 5.8.17. Provide SIPRNet access, or arrange for SIPRNet access at the closest available SIPRNet connection, for all ISSMs and ISSOs within their organization.
- 5.8.18. Ensure development of an integrated and consistent COOP Plan for all mission essential systems, networks, and web sites under their purview and assure its periodic testing.

- 5.9. DLA Field Activity IT Chiefs, Headquarters level Program Managers, Product Managers, and Field Site Project Managers shall:
 - 5.9.1. Activate DLA CERT directed INFOCON actions.
 - 5.9.2. Work closely with the ISSM/ISSO to ensure systems, networks, and web sites are used properly.
 - 5.9.3. Advise the ISSO of security anomalies or integrity deficiencies.
 - 5.9.4. Administer, when applicable, user identification or authentication mechanisms of the system.
 - 5.9.5. Identify security deficiencies and initiate appropriate action to achieve an acceptable security level.
 - 5.9.6. Identify and implement security countermeasures needed to maintain adequate protection.
 - 5.9.7. Identify IT security requirements to include investigative and clearance criteria for inclusion in contracts that comply with the provisions of this directive and references 1.11 and 1.18.
 - 5.9.8. Ensure MOU/MOA are in place for all systems for which DLA provides IT support services.
 - 5.9.9. Ensure MOU/MOA are in place for outsourced IT support services.
- 5.10. Contracting Officers will ensure that specifications identified by DLA Program Managers for IT hardware, software, maintenance services, supplies, or services containing IT security requirements are included in all contracts and Statements of Work (SOWs).
- 5.11. DAA shall:
 - 5.11.1. Certify and accredit all systems, networks, and web sites under their purview and are authorized to suspend operation of a system, network, or web site for which they are responsible when, in their judgment, conditions so warrant.
 - 5.11.2. Accredit systems, networks, and web sites through the DITSCAP process (references 1.8 and 1.9) and provide written acceptance of operational security responsibility, approval for their operation in a designated security mode and at a defined level of risk. Where risks prevent accreditation, DAAs shall either issue statements of Interim Authority to Operate for specified periods of time not to exceed 1 year (pending accreditation) or suspend system operation pending correction of weaknesses.

- 5.11.3. Appoint, in writing, the CA, ISSMs, ISSOs, and user representatives when required, for applicable systems, networks, and web sites.
- 5.11.4. Manage and control access to information systems under their jurisdiction, including access by contractors and individual foreign nationals.
- 5.11.5. Execute MOAs with other DAAs where the authority to accredit does not encompass the entire functional environment, and to effect a secure environment for the development, deployment, operation, and maintenance of the affected and interconnected facilities and/or networks.
- 5.11.6. Identify the level of acceptable risk for a system, network, and web site and determine whether the acceptable level of risk has been obtained. This determination is made by the DAA after a review of the certification package.
- 5.11.7. Ensure that all systems, networks, and web sites under their jurisdiction are assigned the appropriate level of concern and level of robustness to ensure secure operations.
- 5.11.8. Verify that data ownership is established for each system under their jurisdiction and that the system has been assigned a mission category.
- 5.11.9. Incorporate the security requirements outlined in this directive into plans for development, acquisition, accreditation, and operation of systems, networks, and web sites.
- 5.11.10. Ensure, for both developmental and operational environments, a formal access control policy is developed to identify the users and/or user groups who will be permitted access, and at what level, to the systems, networks, and web sites.
- 5.11.11. Grant individual foreign national access to specific classified U. S. networks or systems in accordance with references 1.19 and 1.20.
- 5.11.12. Ensure dissemination of the access control policy to the ISSM/ISSO and to all organizations using or operating the system, network, and web site.
- 5.11.13. Where the developed policy is inadequate or difficult to apply, authorize access via a specific waiver and on a case-by-case basis to files, programs, and databases under their cognizance.
- 5.11.14. Complete appropriate DAA training as identified in the DLA IA Training Plan.

5.12. Certifying Authorities (CA) shall:

- 5.12.1. Support the DAA as the technical expert in the C&A process.
- 5.12.2. Coordinate various activities of the C&A process.
- 5.12.3. Make technical judgments of the system's compliance in both technical and non-technical security features, system features and other safeguards, and ensuring design compliance with security policy.
- 5.12.4. Provide policy interpretation and document system security.
- 5.12.5. Schedule system security test and evaluation (ST&E) in accordance with reference 1.9.
- 5.12.6. Assist the DAA in review and approval of the SSAAs. Provides the DAA with certification status and an accreditation recommendation based on their documented residual risk.
- 5.12.7. Provide oversight for the certification requirements review.
- 5.12.8. Complete DISA-sponsored C&A training.

5.13. Information System Security Managers (ISSM) Shall:

- 5.13.1. Establish and maintain the security for all systems under their jurisdiction including the maintenance of all required safeguards, as specified in accreditation documentation.
- 5.13.2. Identify and include IA requirements in the design/development, acquisition, installation, operation, upgrade, or replacement of all information systems and supporting infrastructures, including security audits, C&A.
- 5.13.3. Provide technical judgment regarding the compliance to DITSCAP requirements of each system, network, and web site. Identify and assess the risks associated with operating each system, network, and web site, coordinate DLA-type certification activities, and consolidate the final C&A package.
- 5.13.4. Ensure that personal information is protected from the unauthorized release which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees, and military personnel: 1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty

phone numbers of units are described in paragraphs C.3.2.1.6.2.2., reference 1.21.

- 5.13.5. Ensure secure remote dial-in procedures are implemented.
- 5.13.6. Ensure coordination and synchronization of IA and CND operations with network management.
- 5.13.7. Consult the IA Technical Framework (IATF) (<http://www.iatf.net>) and published Common Criteria Protection Profiles for guidance regarding common classes of network and system attacks, interoperability and compatibility with the Defense-in-Depth strategy, and IA solutions that should be considered to counter attacks.
- 5.13.8. When required, ensure DLA-owned or operated information systems are enabled to use biometrics for positive access control in accordance with published DoD policy and procedures.
- 5.13.9. Ensure that all DLA systems over which they have cognizance and their interconnections, both internal and external, are managed to continuously minimize community risk and ensure that the protection of one system is not undermined by vulnerabilities of other interconnected systems.
- 5.13.10. Ensure all DLA information systems, services, and applications register the ports and protocols they use in accordance with the established DoD ports and protocols management process.
- 5.13.11. Ensure procedures are in place to coordinate and use outside agencies (e.g., Service CERTS, DISA, and NSA) to conduct external penetration testing and vulnerability assessments of site-specific systems, networks, and web sites. These assessments may include network scans, OPSEC surveys, COMSEC reviews, and Red Team operations. These services, when required, will be requested via DLA IA (J-633) and must be coordinated with DLA CERT.
- 5.13.12. Ensure that all connections to non-GIG information systems, including foreign national and contractor systems, are accomplished in accordance with approved DoD and DLA criteria and coordinated with the DoD CIO and the Intelligence Committee CIO.
- 5.13.13. Ensure that no public domain software products are used in DLA IT systems unless an official requirement is established. Assess the product for IA impacts, and obtain approval for use from the responsible DAA.
- 5.13.14. Ensure that access to DLA information systems is granted to individuals based on a need to know and in accordance

with reference 1.6 for clearances, special access, and IT category designation requirements and qualifications.

- 5.13.15. Ensure that the exchange of unclassified information between DLA and its vendors and contractors requiring IA services is accomplished using approved External Certificate Authorities (ECAs). The ECAs will operate under a process which delivers a level of assurance that meets business and legal requirements as determined by the DoD Comptroller and DoD/DLA General Counsel.
 - 5.13.16. Ensure that all DLA systems are subject to active penetration and other forms of testing used to complement monitoring activities in accordance with reference 1.12 and other laws and regulations.
 - 5.13.17. Ensure mobile code technologies are used in strict accordance with DoD policy in order to reduce the threat to DLA IA systems posed by malicious code.
 - 5.13.18. Perform other ISSM duties as listed in references 1.8 and 1.9.
- 5.14. ISSOs shall:
- 5.14.1. Report to the local ISSM for guidance and direction and will ensure compliance with this policy directive for their field site commander or staff office.
 - 5.14.2. Review all proposed system changes to determine if the secure operation of the system, network, or web site will be affected. Formally endorse all completed changes, certifying that the prevailing security protection has not been weakened.
 - 5.14.3. Inform the ISSM (IT Chief when no ISSM is assigned), and the DAA of minor or major changes that may affect the integrity of the system being modified.
 - 5.14.4. Develop and maintain an Information System Security Plan (ISSP) as defined in reference 1.2 for each system, network, or web site under his or her jurisdiction.
 - 5.14.5. Ensure that every system in his or her jurisdiction is operated, used, maintained, and disposed of in accordance with the system's SSAA and local security policies and practices.
 - 5.14.6. Coordinate security measures including analysis, testing, evaluation, verification, accreditation, and review of each site-specific system, network, and web site at the appropriate classification level within the commands network structure.
 - 5.14.7. Provide an IA monitoring and testing capability in accordance with reference 1.9.

- 5.14.8. Within ISSO lines of authority (DAA via ISSM/IT Systems Chief), enforce IA policies and safeguards on all personnel having access to each system for which the ISSO has cognizance.
- 5.14.9. Administer, when applicable, user identification or authentication mechanisms of the system.
- 5.14.10. Maintain a plan for site security improvements and progress towards meeting full accreditation and/or continued improvement in risk mitigation.
- 5.14.11. Recommend the criticality and sensitivity levels for each site-specific system, network, or web site.
- 5.14.12. Ensure users and system support personnel have the required security clearances, authorization and need-to-know; are indoctrinated; and are familiar with internal security practices before access to IT system is granted.
- 5.14.13. Ensure that audit trails are turned on and reviewed periodically. In an adjunct capacity to the DLA CERT, review firewall and intrusion detection logs for their respective command or facility.
- 5.14.14. Evaluate known vulnerabilities to ascertain if additional safeguards are needed.
- 5.14.15. Report all non-administrative security incidents to local ISSM and DLA CERT.
- 5.14.16. Develop and maintain an effective account management program including the assignment and control of passwords and the implementation and maintenance of a comprehensive PKI Program.
- 5.14.17. Maintain liaison with DLA, DoD, and non-DoD counterparts to track developments in the computer security area and keep current with pertinent computer security issues.
- 5.14.18. Submit reports on the IA posture of the information systems as required by the local ISSM, IT System Chief, and local DAA as defined in DLA/DoD policy (reference 1.2).
- 5.14.19. Establish a program consistent with reference 1.19 for disposing of information systems components (hard drives and other storage medium including removable disk packs, sealed disk drives, magnetic Bernoulli cartridges, optical disks, and optical tapes) when being disposed of outside DoD.
- 5.14.20. Additionally, perform ISSO duties as listed in references 1.8 and 1.9.

5.15. System Administrators (SA) shall:

- 5.15.1. Work closely with the ISSO to ensure the system is used properly.
- 5.15.2. Assist the ISSO in maintaining system configuration controls and need-to-know information protection mechanisms.
- 5.15.3. Advise the ISSO of security anomalies or integrity deficiencies.
- 5.15.4. Administer, when applicable, user identification, or authentication mechanisms of the system.
- 5.15.5. Perform system backups, software upgrades, and system recovery, including the secure storage and distribution of backups and upgrades.
- 5.15.6. Perform other SA duties as listed in references 1.4 and 1.5.

5.16. TASOs shall:

- 5.16.1. Act as the representative of the ISSO to the users within their designated area.
- 5.16.2. Assist users in understanding and complying with systems security procedures to protect computer workstations and determine adequate protection criteria for the information processed.
- 5.16.3. Be the user focal point for administration and access control mechanisms (e.g., user identifications, passwords, and certificates). Maintain site security checklists for physical security (e.g., door locks, alarm systems) in accordance with site physical security policies.
- 5.16.4. Keep a log of all computer access control assignments (i.e., accounts) granted to each employee.
- 5.16.5. Delete user's system permission when access to a system is no longer required.
- 5.16.6. Document and report all computer system viruses, security violations, and incidents to ISSO.
- 5.16.7. Serve as trusted agent when needed.
- 5.16.8. Solicit guidance from the ISSO when necessary.
- 5.16.9. Assist ISSO in related matters.

5.17. RAs and LRAs shall:

5.17.1. Ensure compliance with PKI policy addressed in this directive for his or her DLA Field Activity Commander or staff office.

5.17.2. Perform RA or LRA duties as listed in references 1.4 and 1.5.

5.18. Authorized Users shall:

5.18.1. Comply with DLA IA policy, practices, and procedures.

5.18.2. Immediately report all known or suspected IA incidents, potential threats, and vulnerabilities in accordance with established procedures.

5.18.3. Observe regulations and guidance governing the secure operations (e.g., protection of passwords) and authorized use of an information system.

6. EFFECTIVE DATE. This publication is effective immediately.

BY ORDER OF THE DIRECTOR.

RICHARD J. CONNELLY
Director
DLA Support Services

Enclosures

Enclosure 1, References

Enclosure 2, Definitions

Coordination: J-1, J-3, J-8, J-9, DSS, DG, DI

This page intentionally left blank.

References

- 1.8. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), dated December 30, 1997.
- 1.9. DoD Manual 8510.1M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, dated July 31, 2000.
- 1.10. Assistant Secretary of Defense (C3I) memorandum "Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," dated November 7, 2001.
- 1.11. NSTISSP No. 11, National Information Assurance Acquisition Policy, dated January 2000.
- 1.12. DoD Directive 5200.28, Security Requirements for Automated Information Systems, dated March 21, 1988.
- 1.13. Computer Security Act of 1987 (PL 100-235) dated January 8, 1988.
- 1.14. OMB Circular A-130, "Management of Federal Information Resources," Appendix III, February 8, 1996
- 1.15. Clinger-Cohen Act of 1996 (Public Law 104-106) dated June 2, 1997.
- 1.16. National Institute of Standards and Technology (NIST) Special Publication 800-16, "Information Technology Security Training Requirements," dated April 1998.
- 1.17. DLA IA Training Plan, dated June 2001.
- 1.18. DoD 5200.1-R, Information Security Program, June 1986.
- 1.19. DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, June 16, 1992.
- 1.20. DoDD 5230.2, Visits, Assignments, and Exchanges of Foreign Nationals, August 17, 1998.
- 1.21. DoDD 5400.7, Freedom of Information Act, September 29, 1997.
- 1.22. Executive Order 12958, Classified National Security Information, 20 April 1995
- 1.23. DLAR 4710.1, "Management of Federal Information Processing (FIP) Resource Acquisitions," dated September 8, 1992.
- 1.24. ASD (C3I) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated May 29, 2001.

- 1.25. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary (Revision 1), dated September 2000.
- 1.26. OSD Memorandum, "Use of DoD Information and Telecommunications Systems," dated February 1, 1997.
- 1.27. DoD Manual 5200.28M, "ADP Security Manual," dated January 1973
- 1.28. Executive Order, E.O. 12958, dated April 17, 1995.
- 1.29. DoDD 4604.6, Communications Security (COMSEC) Monitoring and Recording, dated June 26, 1981.
- 1.30. Deputy Secretary of Defense Policy Memorandum, "Web Site Administration," dated December 7, 1998.
- 1.31. Web Site Administration Policies and Procedures, dated November 25, 1998.
- 1.32. DISA WASHINGTON DC message 021730Z NOV 99, subject: DISN Unclassified But Sensitive Internet Protocol Router Network Connection Approval Process.
- 1.33. DLA CIO letter 99-5, Information Operations Condition (INFOCON), dated May 6, 1999.
- 1.34. DLA IA Program Management Plan, dated January 2002.
- 1.35. DLAD 8500.11, DLA Internet Management, dated June 25, 2001.
- 1.36. DLAI 8500.12, Enclave Boundary Defense, dated February 25, 2002.

DEFINITIONS

1. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
2. Availability. Timely, reliable access to data and information services for authorized users.
3. Blue Team. Cooperative effort by an interdisciplinary team to review, assess, and document vulnerabilities as a means to improve the security posture of information systems.
4. Computer Emergency Response Team (CERT)/Computer Incident Response Team (CIRT). Team of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services; an operational organization for rapid response to both deployed and installation based Service forces.
5. Certification Authority (Certifier) (CA). Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying, and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final C&A package.
6. Classified Information. Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
7. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
8. CND Service (CNDS). A DoD certified service provided or subscribed to by owners of DoD information systems and/or computer networks in order to provide CND situational awareness; implement CND protect measures; monitor and analyze in order to detect unauthorized activity; and implement CND operational direction. A Computer Emergency or Incident Response Team (CERT/CIRT), located within a Network Operations and Security Center (NOSC), commonly provides CNDS.
9. Communications security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Includes crypto security, transmission security, emission security, and physical security of COMSEC materials and information.
10. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

11. Defense-in-Depth. Defense-in-Depth is a security approach that uses layers of IA technical and non-technical solutions to establish an adequate IA posture for the DLA-wide systems, networks, and web sites. Defense-in-Depth focuses on the local computing environments (or enclaves), enclave boundaries, networks that link enclaves, and supporting infrastructures and integrates the capabilities of people, operations and technology to establish multi-layer, multi-dimensional protection of networked systems
12. Designated Approving Authority (DAA). The designated authority at the local (field site or headquarters) level with the authority to formally assume responsibility for site specific (unique) systems, networks, or web sites operating at an acceptable level of risk.
13. DLA Enterprise. The Director, DLA, the headquarters Components, field sites, and all other DLA organizations (to include commercial activities serving in an operational capacity for DLA).
14. DLA Program Manager/Product Manager or IT Systems Chief. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of an IA system.
15. Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that have access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or mission and may also contain multiple networks. Enclaves may be logical, such as an operational area network, or be based on physical location and proximity. The enclave encompasses the network layer, the host, and the applications layer.
16. Encryption. (a) End-to-end encryption addresses the protection or information passed in a telecommunications system by cryptographic means, from point of origin to point of destination; (b) Link encryption provides the protection of information applied in a link of a communications system so that all information passing over the link is encrypted.
17. Encryption Algorithm. A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by the application of a key.
18. External Certificate Authority (ECA). An external (outside DoD) agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DOD entities. Operating requirements for ECAs must be approved by the DoD CIO, in coordination with the DOD Comptroller and the OSD General Counsel.
19. For Official Use Only (FOUO). Unclassified official information of a sensitive, proprietary, or personally private nature which must be protected against unauthorized public release pursuant to

exemptions 2 through 9 of the Freedom of Information Act (FOIA) as implemented by DLAR 5400.14.

20. Global Information Grid (GIG). The global interconnected capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information for all DoD warfighters, policy makers, and support personnel.
21. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporation of protection, detection, and reaction capabilities.
22. IA Vulnerability Alert (IAVA). The comprehensive distribution process for notifying Commanders in Chief, Services, and Agencies (C/S/A) about vulnerability alerts and countermeasures information.
23. Information Operations Condition (INFOCON). INFOCON is a comprehensive defense posture and response system based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack.
24. INFOCON Advisory Committee. Comprised of an individual from J-6341, J-633, the DLA CERT, and DSS-S, the INFOCON Advisory Committee meets whenever a change to the INFOCON level is recommended.
25. Information System. The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.
26. Information System Security (INFOSEC). Protection of information systems against unauthorized access to information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.
27. Information Systems Security Manager (ISSM). The individual responsible for a program, organization, system, or enclave's IA Program; principal advisor on computer security matters.
28. Information Systems Security Officer (ISSO). An individual responsible to the DAA and ISSM for ensuring that the appropriate operational IA posture is maintained for a system, program, or enclave from design to disposal.
29. Information System Security Policy (ISSP). The ISSP identifies security requirements, objectives, and policies implemented to safeguard the site or system in a prescribed operational configuration, to include requirements for system redundancy and data backup and risk management decisions. Contingency plans must be developed and tested to prepare for emergency response, backup

operations, and post-disaster recovery. This policy document must become part of the SSAA for each system, network, or web site required by the DITSCAP.

30. Information Technology (IT) position category. The IT position identifies the level of access required or available in the execution of an individual's duties.

30.1. IT-I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a security program; has major responsibility for the direction, planning, and design of a computer system, including hardware and software; or can access a system during operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize significant personal gain.

30.2. IT-II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher Authority of the IT-I category to ensure integrity of the system.

30.3. IT-III positions. All other positions involved in computer activities not covered in IT-I and IT-II paragraphs described above.

31. Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

32. Level of Concern. A rating assigned to an information system that indicates the extent to which protective measures, techniques, and procedures must be applied. DoD has three levels of concern:

32.1. High: Information systems that require the most stringent protection measures and rigorous countermeasures.

32.2. Medium: Information systems that require layering of additional safeguards above the DoD minimum standard (Basic).

32.3. Basic: Information systems that require implementation of DoD minimum standards.

33. Level of Robustness. The characterization of strength of a security function, mechanism, service or solution, and assurance (or confidence) that is implemented and functioning correctly to support the level of concern assigned to a particular information system. DoD has three levels of robustness:

33.1. High: Security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures.

- 33.2. Medium: Security services and mechanisms that provide layering of additional safeguards above the DoD minimum (BASIC).
- 33.3. Basic: Security services mechanisms that equate to good commercial practices.
34. Malicious mobile code. Malicious mobile code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources.
35. Mission categories. All DLA systems, networks, and web sites will be categorized within one of the following categories:
- 35.1. Mission Critical (Mission Category I): Systems handling information determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a Category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Category I systems require the most stringent protection measures.
- 35.2. Mission Support (Mission Category II): Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Category II systems require additional safeguards beyond best practices to ensure adequate assurance.
- 35.3. Administrative (Mission Category III): Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.
36. Mobile code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, VBScript, and ActiveX. There are three (3) categories of mobile code.

36.1. Category 1: Category 1 mobile code technologies exhibit a broad functionality allowing unmediated access to workstation, host, and remote system services and resources. Category 1 mobile code has known security vulnerabilities with few or no countermeasures once they begin executing. Execution of Category 1 mobile code typically requires an all or none decision; either execute with full access to all system resources or don't execute at all. Category 1 mobile code may be used in DLA information systems only when the mobile code is signed with a DoD-approved PKI signing certificate or when the DLA CIO approves alternate commercially available code signing certificates.

36.2. Category 2: Category 2 mobile code technologies have full functionality, allowing mediated or controlled access to workstation, host, and remote system services and resources. Category 2 mobile code may have known security vulnerabilities but also have known fine-grained, periodic, or continuous countermeasures or safeguards. Category 2 mobile code technologies may be used in DLA information systems if the mobile code is obtained from a trusted source over an assured channel.

36.3. Category 3: Category 3 mobile code technologies support limited functionality, with no capability for unmediated access to workstations, hosts, and remote system services and resources. Category 3 mobile code technologies may have a history of known vulnerabilities, but also support fine-grained, periodic, or continuous security safeguards. Category 3 mobile code technologies may be used in DLA information systems.

37. Network: IS-implemented with a collection of interconnected network nodes. A group of computers that can communicate with each other, share peripherals (such as hard disks and printers), and access remote hosts or other networks. For SSAA status reporting, interfacing networked are those networks outside the accreditation boundary which either are "connected to" or are "to be connected to" the information systems(s) being certified and accredited.
38. Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
39. Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems; (b) determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in a time to be useful to adversaries; (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
40. Personal Electronic Device (PED). Personal Digital Assistants (PDAs), palmtops, hand-held computers, cell phones, two-way pagers, wireless e-mail devices, and audio and video recording devices.

41. Portable Electronic Devices: Laptops, cellular devices, land mobile radios, mobile satellite systems, audio/video recording devices, scanning devices, messaging devices, personal digital assistants, and any other devices capable of storing, processing, or transmitting information operating in either or both wired and wireless modes.
42. Privileged User. An individual who has access to system control, monitoring, or administrative functions.
43. Public Key Infrastructure (PKI). Framework established to issue, maintain and revoke public key certificates accommodating a variety of security technologies, including the use of software.
44. Red Team. Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems.
45. Risk Management. Identifying risk as a function of the probability of threats measured against vulnerabilities in terms of the values of the assets in question. A basic tenet is that of shared risk -- risk assumed by one is a risk shared by all. Safeguards (such as Firewalls, Intrusion Detection Systems (IDS), and Public Key Infrastructure (PKI) certificates) ensure that DLA information and information systems maintain acceptable levels of availability, integrity, and confidentiality of information resources.
46. Rules of Behavior. The clearly delineated responsibilities and expected behavior of all individuals with access to the system. Based upon the acceptable level of risk, such rules should be only as stringent as necessary and should provide adequate security for the system and the information it contains. They shall also be clear about the consequences of behavior not consistent with the rules.
47. Sensitive information. Any information the loss, misuse, unauthorized access to, or modification of which could adversely affect U.S. national interests, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.
48. Site critical system. Any system which, if down, would require the filing of a Situation Report (SITREP).
49. Site-specific (Unique) system. A set of interrelated components consisting of mission, environment, and architecture operating in a unique or site-specific configuration. DLA systems addressed in this category are those administrative systems that are specifically designed to operate with unique characteristics at one DLA site.
50. System Security Authorization Agreement (SSAA). A formal agreement among the DAA, the Certifier, User Representative, and Program Manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document

certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

51. Terminal Area Security Officer (TASO). Assists the ISSO to ensure compliance with security procedures in an assigned remote terminal area. TASOs coordinate with the ISSO to implement physical and AIS security requirements for devices and remote terminal areas processing sensitive/unclassified or classified information.
52. User representative. The individual(s) or organization that has been assigned by the DAA to represent the user or user community in the definition of IA requirements.
53. Web Site. A collection of web files on a particular subject that includes a beginning file called a Home page. The home page usually includes the URLs and/or IP addresses for successive pages and related websites. The web server environment includes the physical computing resources, including servers, software, network, communication, security, and peripheral devices that provide the platform upon which web sites are made available to users through the internet. For SSAA status reporting, all public and private web servers supporting system or site requirements should be identified. 'Interfacing web sites' are those web sites outside the accreditation boundary either connected to, or are to be connected to, the information system(s) being certified and accredited.

NOTE. Other IA terms are as defined in reference 1.20.