Audit Report

IDENTIFICATION AND AUTHENTICATION POLICY

Report No. D-2000-058 December 20, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

To suggest ideas for or to request audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
AI-26	Administrative Instruction 26
AIS	Automated Information System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
NIST	National Institute of Standards
OSD	Office of the Secretary of Defense
WHS	Washington Headquarters Services

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

December 20, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on Identification and Authentication Policy (Report No. D-2000-058)

We are providing this report for review and comment. We conducted the audit in response to your office's request. We considered your comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments were generally responsive. For followup purposes, we request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments by February 4, 2000, to indicate estimated completion dates for the agreed-upon actions on Recommendations 1 and 2.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Jerry Hall (703) 604-9098 (DSN 664-9098) (jerry@dodig.osd.mil) or Mr. George Cherry (703) 604-9018 (DSN 664-9018) (hgcherry@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2000-058 **December 20, 1999**
(Project No. 9AS-0048)

Identification and Authentication Policy

Executive Summary

Introduction. In May 1999, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), alerted systems owners and users to the potential of increased vulnerabilities as a result of year 2000 testing, evaluation, and renovation processes that exposed the DoD information systems and networks to a growing and increasingly sophisticated variety of information warfare threats. Further, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) requested that all personnel using DoD systems comply with the Office of the Secretary of Defense Administrative Instruction 26, Chapter 11, Section 5.1.1, that identifies the Office of the Secretary of Defense policy on identification and authentication controls.

Objectives. The overall audit objective was to evaluate the adherence of system users to DoD information systems security policy, during and after year 2000 conversion efforts. Specifically, we were to determine the security procedures used for contractor support of year 2000 efforts, using as criteria the requirements of Administrative Instruction 26, Chapter 11, and Section 5.1.1. We will accomplish the audit objective in two phases. In this phase, we reviewed current DoD Component policies on the use of identification and authentication controls to access information systems. In the second phase, we will review procedures for identification and authentication for year 2000 renovated systems at selected locations.

Results. DoD policy covering access controls over information systems has not been updated since March 1988 and has not kept pace with changing defense information infrastructure and technology advancements. Service, Defense Agencies, and Office of the Secretary of Defense policies governing the use of identification and authentication as a means of controlling access to information systems vary significantly. Until the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) updates information security policies or issues other policy guidance that specifically establishes uniform security requirements, DoD efforts to reduce vulnerability and exposure of the Defense Information Infrastructure will be hampered. See the finding section of the report for a discussion on the audit results.

Summary of Recommendations. We recommend that the Assistance Secretary of Defense (Command, Control, Communications, and Intelligence) immediately provide specific interim policy guidance to establish minimum security requirements covering identification and authentication and accelerate the reissuance of a governing DoD Directive.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred, stating that the Infrastructure and Information Assurance Directorate does not take exception to the recommendations.

Also, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that Administrative Instruction 26 is only applicable to the Office of the Secretary of Defense and not to any of the components examined. Therefore, it is not surprising that all of the 18 requirements in Administrative Instruction 26 are not fully covered by all other policies.

Additionally, the Assistant Secretary stated that the draft identification and authentication policy does not provide detailed identification and authentication controls like those found in Administrative Instruction 26. The approach taken in the draft policy is to allow the DoD components discretion in implementation as long as they satisfy policy requirements for identification and authentication and interoperability.

A discussion of the management comments is in the Findings section of the report and the complete text is in the Management Comments section.

Audit Response. The Assistant Secretary's comments were generally responsive, although they lacked specificity on estimated dates by which the actions will be completed. The Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [now the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)], issued a memorandum on "Year 2000 (Y2K) and the Importance of Adherence to Department of Defense (DoD) Information Security Policy," May 5, 1999, and asked that all personnel using DoD systems comply with the guidance in Administrative Instruction 26, Chapter 11, particularly Section 5.1.1. Rather than argue with the applicability of the citation in the May 5, 1999, memorandum, we used the content of Administrative Instruction 26 to measure the uniformity of requirements between security policies of various DoD Components. The audit results illustrate the wide range of disparity between the various policies and highlight the immediate need for a uniform set of DoD requirements for identification and authentication controls. If component policies vary in stringency, the weaker policies may well be an inherent causal factor that increases vulnerabilities. We are not advocating a policy on technological solutions, but rather a policy that outlines DoD expectations of minimum controls and protection. It is precisely because of the decentralized establishment of nonuniform policy requirements that an overall DoD information assurance management strategy continues to be inadequately implemented. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide comments on the final report, indicating when the agree-upon actions related to Recommendations 1 and 2 will be completed, by February 4, 2000.

Table of Contents

Executive Summary i

Introduction

Background 1
Objective 3

Finding

Information Systems Security Policy on Identification and Authentication 4

Appendixes

A. Audit Process
Scope 17
Methodology 17
Summary of Prior Coverage 17
B. Chronology of Actions Relating to Recommendation Made in Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems." 19
C. Report Distribution 21

Management Comments

Assistant Secretary of Defense (Command, Control, Communications And Intelligence) 23

Introduction

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C^3I]) asked the Inspector General, DoD, to monitor DoD Components adherence to the Office of the Secretary of Defense (OSD) information security requirements, specifically those addressing identification and authentication controls, OSD Administrative Instruction 26 (AI-26), as part of ongoing audits. Additionally, the ASD(C^3I) staff requested a comparison of the status of Service Component and Defense Agency policies with the requirements in AI-26.

Background

Control Risks. There has been a significant increase in computer system intrusions. This has highlighted the vulnerability of information systems. In February 1997, the General Accounting Office designated information security as a high-risk area because weaknesses in information security could cause critical operations to be highly vulnerable to waste, fraud, abuse, and mismanagement. DoD Annual Statements of Assurance for fiscal years 1995 through 1998 classify information systems security as a material management control weakness.

Office of the Assistant Secretary of Defense. The ASD(C^3I) serves as the Chief Information Officer and senior information security official for DoD. He also is the principal advisor for C^3I, information management, information operations, and other functions.

DoD Information Security Policy. In a memorandum on "Year 2000 (Y2K) and the Importance of Adherence to Department of Defense (DoD) Information Security Policy," dated May 5, 1999, the ASD(C^3I) alerted information system owners and users of the potential increased vulnerabilities as a result of year 2000 testing, evaluation, and renovation processes. As a precaution ASD(C^3I) requested that all personnel using DoD systems comply with the requirements in AI-26, Chapter 11, Section 5.1.1, "Identification and authentication."

Administrative Instruction 26. The Washington Headquarters Services (WHS) has prepared security policy and procedures governing the certification, accreditation, and operation of information systems in AI-26, "Information Systems Security," March 1999. Although AI-26 is still in draft, the Director, WHS, in a memorandum dated April 22,1999, established AI-26 as official OSD policy for information systems security.

Applicability. AI-26, Chapter 11 applies to:

> . . . information systems directly supported by OSD Components. Department of Defense (DoD) civilians, contractors, technical, and military personnel who use, access, operate, and maintain OSD information systems will follow this instruction. This AI (AI-26)

provides uniform guidance to all organizations of the OSD and other organizations (Task Force, Presidential Commissions, Panel, etc.,) that receive administrative support from Washington Headquarters Services (WHS), referred to collectively in this document as the OSD Components.

AI-26 does not apply to the Service Components or the major Defense Agencies: Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), and the Defense Finance and Accounting Agency (DFAS).* The DoD Components are responsible for developing their own policies and procedures.

Chapter 11 Section 5.1.1. Chapter 11 Section 5.1.1 of AI-26 describes 18 identification and authentication requirements to control access to automated information systems. These controls include procedural requirements for users and system administrators as well as password and system specifications. See the finding for a discussion of the identification and authentication requirements.

Access Controls. Access controls limit or detect inappropriate access to computer data, programs, facilities, and equipment to protect against unauthorized modification, disclosure, loss, or impairment. Access controls include physical protections, such as gates and guards, and logical controls, which are built into software to authenticate users through passwords or other means and to restrict access.

Identification and Authentication. Identification and authentication, typically the login process, are the primary logical access controls. Identification is the process where individuals identify themselves to a system as a valid user. Authentication is the process where the system verifies that the user has the right of access. User identifications and passwords, because of cost efficiency and ease of implementation, are the most common identification and authentication methods. However, because of vulnerability to interception and inadvertent disclosure, passwords are also the weakest of the identification and authentication methods.

*The Service Components and major Defense Agencies will be referred as DoD Components throughout the remainder of the report.

Objective

The overall audit objective was to evaluate the adherence of system users to DoD information systems security policy, during and after year 2000 conversion efforts. Specifically, we were to determine security procedures used for contractor support of year 2000 efforts, using as criteria AI-26, Chapter 11, and Section 5.1.1. We will accomplish the audit objective in two phases. In this phase, we reviewed current DoD Component policies on the use of identification and authentication controls to access information systems In the second phase, we will review procedures for identification and authentication for year 2000 renovated systems at selected locations. See Appendix A for a discussion of audit scope, methodology, and a discussion of prior coverage.

Information Systems Security Policy on Identification and Authentication

DoD Component and OSD policies governing the use of identification and authentication as a means of controlling access to information systems have significant variations. Nonuniform practices proliferated because DoD information systems security policies became out of date as technology changed and the ASD(C^3I) did not issue standard security policy to respond to the changing technology as well as to consolidate existing policies. From 1988 to the present, DoD Components produced their own individual policies or operated under older procedures that were neither consistent nor necessarily within the bounds of the ASD(C^3I) intent. Until the ASD(C^3I) updates existing information security policies or issues other policy guidance that specifically establishes uniform security requirements, DoD efforts to reduce the vulnerability of the information infrastructure will be hampered.

DoD Policy

Existing Policy. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" March 21, 1988, is the current DoD policy governing automated information systems security requirements. On the subject of access controls, Section E3.1.1.2., states:

> There shall be in place an access control policy for each AIS. It shall include features and/or procedures to enforce the access control policy of the information within the AIS. The identity of each user authorized access to the AIS shall be established positively before authorizing access.

The regulation does not specifically discuss identification and authentication, nor does it provide detailed guidance on the use of passwords. The regulation does provide broad guidance on computer security and leaves the details for the DoD Components to work out.

Draft DoD Security Policy. The final policy on specific DoD security requirements has been delayed and the ASD(C^3I) is in the process of consolidating and revising overarching policies.

Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997, recommended, among other remedies, the revision of ineffective and outdated policies and procedures to improve inadequate security safeguards and practices for DoD automated information systems. In response to the report, OSD stated that DoD Instruction 5200.28, or subsequent versions of an overall DoD information security policy, would be updated in October 1997. The October date was revised to July 1999. The guidance has not yet been issued. (Inspector General, DoD, Report PO 97-049 is discussed further

in Appendix A of this report. A chronology of events surrounding the resolution of this audit is presented in Appendix B.)

We also reviewed the section covering identification and authentication for password controls in the ASD(C^3I) draft "Guidance and Policy for Department of Defense Information Assurance," Version J-1, August 12, 1999, and the ASD(C^3I) coordination draft documents on the "Global Information Grid (GIG) Policy Guidance," October 1999. This guidance did not provide detailed identification and authentication controls.

Access Control Policies - DoD Wide

In addition to the DoD draft policy discussed, the Army and Navy have draft policies in process that are being upgraded to meet individual service needs. The current official policies of DoD and the DoD Components are identified below.

Table 1. Current Official Information Security Policies of DoD, the Services, and Defense Agencies

	Date	Reference	Title
DoD	March 21, 1988	DoD Directive 5200.28	Security Requirements for Automated Information Systems (AISs)
Army	February 27, 1998	Army Regulation 380-19	Information Systems Security
Navy	August 3, 1982	OPNAVINST 5239.1A	Department of the Navy Automatic Data Processing Security Program
Air Force	June 1, 1998	Air Force Manual 33-223	Identification and Authentication
Defense Information Systems Agency	July 9 1996	DISA Instruction 630-230-19	Automatic Data Processing Information Systems Security Program
Defense Finance and Accounting Service	October 15, 1998	DFAS Regulation 8000.1R, Volume 1	Information Management Policy Instructional Guidance
Defense Logistics Agency	June 9, 1993	DLA Regulation 5200-17	Defense Logistics Agency Security Requirements for Automated Information and Telecommunications Systems

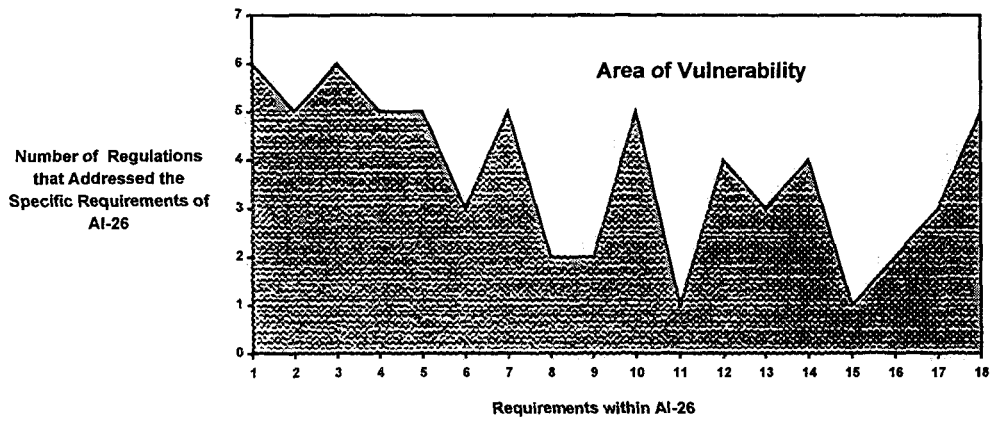
While the Air Force, Army, and DFAS are using regulations published in 1998, the controlling DoD Directive is dated 1988. Furthermore, the applicable Navy regulation is 17 years old.

Identification and Authentication

ASD(C^3I) has requested that all personnel using DoD systems comply with the requirements in AI-26, Chapter 11, Section 5.1.1, "Identification and Authentication."

In response, we reviewed the seven documents identified in Table 1 and matched the contents to the 18 requirements in AI-26. Figure 1 identifies the range of vulnerability due to uncovered requirements within existing polices and procedures. For example, Figure 1 shows that six of the seven DoD documents address requirement 1, system access. An area of vulnerability exists for the DoD component that has not addressed a requirement.

Figure 1. Conformity of Existing DoD Regulations with the Requirements of AI-26, Chapter 11, Section 5.1.1



Existing DoD and DoD Component policies vary significantly from the requirements in AI-26. All of the 18 requirements in AI-26 are not fully covered by all other policies.

A summary of how effectively DoD and each DoD Component policy addresses the 18 requirements follows.

Requirement Number 1—System Access. The user is required to enter a login before being allowed access to the system. This requirement appears in all but the Navy policy

Requirement Number 2—Password Format. Passwords must be at least eight characters long and consist of alpha and numeric characters. Only, the Army and the Air Force guidance have identical requirements. DLA requires that the password consist of a minimum of six alphanumeric characters with at least one embedded number or special character. DFAS and DISA require that the password contain a minimum of six characters, but do not require alphanumeric format restriction. DoD and Navy policies do not mention password format.

Requirement Number 3—User Validation. Passwords are to be validated each time a user accesses the system. All but the Navy address user validation.

Requirement Number 4—Password Protection. Passwords must not be displayed at any terminal or printer. Army, Navy, Air Force, and DFAS policies prohibit display of passwords. DLA prohibits any intentional acts that produce conditions likely to lead to password compromise. DISA and DoD policies do not mention this requirement.

Requirement Number 5—User Maintenance. Passwords must be changed at least every 90 days. Air Force policy states that passwords should be changed at least every 90 days. DISA, DLA, DFAS, and the Army require passwords to be changed every 180 days. However, the Army does specifically require passwords for classified systems to be changed every 90 days. DoD and Navy policies do not address the requirement for password changes.

Requirement Number 6—Encryption. Encryption of electronic stored passwords is required. The Navy, Air Force, and DLA stated that passwords must be stored in an encrypted form to prevent system vulnerability. DoD, Army, DFAS, and DISA policies do not address the issue of electronically encrypting passwords.

Requirement Number 7—Authentication Failures. System users are limited to five consecutive authentication failures after which access to the desktop system is automatically deactivated for a minimum of 20 minutes and an audit trail record is created. Air Force, DFAS, and DISA policies are more stringent. Each requires their systems to lock out users after three unsuccessful log-on attempts. Navy and DLA policies do not identify how many unsuccessful attempts the user is allowed. Navy and DLA policies require the capability to lock out users after an unspecified number of unsuccessful attempts. DISA policy requires lockout after two unsuccessful attempts but only for mission-critical systems or systems processing information classified higher than secret. Only the Air Force policy specifically requires an audit trail containing a record of unsuccessful log-on attempts. Army and DoD policies do not address this issue.

Requirement Number 8—User Password History. A password history should be maintained for one year. Only Air Force and DISA policies include any password history retention requirements. DISA policy requires audit records to

be retained for at least one year. The Air Force requires a retention period of a minimum of 6 months to prevent users from using former passwords.

Requirement Number 9—Memorizing Passwords. Users should memorize their passwords. The Air Force policy matched AI-26 exactly and DLA mentioned that forgetting a password would be considered a security incident. DoD, Army, Navy, DISA, and DFAS did not specifically address the issue of memorization.

Requirement Number 10—Disclosure of Passwords. Under normal circumstances, users do not disclose their personal passwords to anyone. Also, disclosing a personal classified system password to anyone without a valid clearance and need-to-know constitutes a security violation. DISA and DLA classify the intentional sharing of a password as a security violation. Army, Air Force, and DFAS prohibit the disclosure of unauthorized disclosure of passwords. Navy and DoD policies do not mention disclosure of personal passwords.

Requirement Number 11—Shared Passwords. A shared password must be changed as soon as possible. Only Air Force policy specifically requires a password to be changed immediately after shared access is no longer required. DoD, Army, Navy, DLA, DFAS, and DISA do not mention this requirement.

Requirement Number 12—Compromised Passwords. The user must immediately notify the systems administrator or information system security officer if it is believed that a password has been compromised. Army and DISA policies require prompt or immediate notification in the event of password disclosure. In DLA, the responsibility of reporting compromised security violations is the maintainer's. DFAS requires users to know how to report an incident of unauthorized or attempted unauthorized entry into the system. DoD, Navy, and Air Force policies do mention this requirement.

Requirement Number 13—Unclassified System Access. Systems administrators should share unclassified system access passwords only when necessary. When possible unclassified system access passwords should be sealed in a Standard Form 700 or plain envelope and protected similar to classified system passwords. Army, Air Force, and DFAS policies require handling, storing or protection of passwords. DoD, Navy, DLA, and DISA do not mention this requirement.

Requirement Number 14—Classified System Access. Systems administrators will make classified system passwords available to other system administrators only during an emergency. This will be accomplished by storing a copy of the password in a secure container. DoD, Army, and Air Force policies address storage and sharing of classified system passwords. DFAS policy requires the system to protect password files so that they cannot be accessed by any user/administrator. Navy, DLA, and DISA policies do not mention this requirement. None of the policies address sealing the password in a SF 700 and storage in a manner similar to classified system passwords.

Requirement Number 15—Factory Issued Identifiers or Passwords. All factory set, default, or standard user IDs and passwords are removed or changed. Navy policy specifically requires the changing of embedded passwords that come with vendor software. DoD, Army, Air Force, DLA, DFAS, and DISA do not mention this requirement.

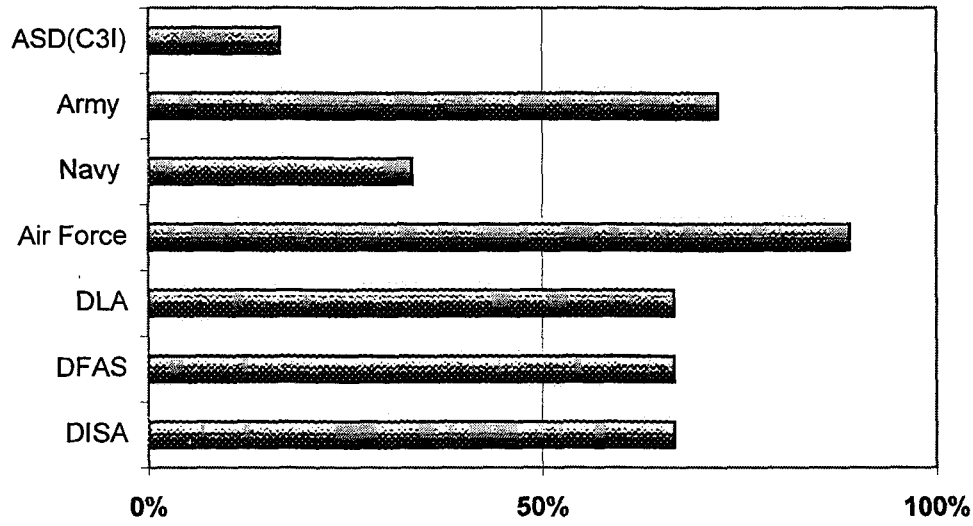
Requirement Number 16—Conditions Requiring Password Changes. Passwords are changed when compromised, possibly compromised, forgotten, or when they appear on an audit document. The Air Force and DFAS policies specifically require compromised passwords to be changed. DoD, Army, Navy, DLA, and DISA policies do not mention this requirement.

Requirement Number 17—Disabling Passwords. Passwords are disabled if a user no longer requires access to the system. Army policy requires retirement of passwords and Air Force policy requires removal of user IDs when access is no longer required. DISA policy states that the user should notify the terminal area security officer or information system security officer when access is no longer required, but DISA policy does not address disabling the password or access. DoD, Navy, DLA, and DFAS do not mention this requirement.

Requirement Number 18—Classification and Control of Passwords. Passwords are classified and controlled at the highest level of the information accessed or the classification level of the system. Air Force, DLA, and DISA policies meet the standards as outlined in AI-26. The Army and Navy designate the responsibility for managing passwords to the information system security officer and the automatic data processing system security officer. DoD and DFAS policies do not mention this requirement.

In summary, Air Force and Army policies cover the AI-26 requirements more closely than Navy and DoD policies. Figure 2 depicts the degree of conformance for DoD and DoD Components to the requirements in AI-26.

Figure 2. Degree of Conformity of DoD Component Policies with AI-26, Chapter 11, Section 5.1.1



Other Identification and Authentication Controls

Although the ASD(C^3I) asked that we use the AI-26, Chapter 11, Section 5.1.1, in the process of reviewing other applicable DoD and DoD component policies, we identified other controls that merit consideration in development of a uniform DoD policy. Table 2 discusses identification and authentication controls not addressed in AI-26, Chapter 11, Section 5.1.1.

Table 2. Identification and Authentication Controls not Addressed in AI-26, Chapter 11, Section 5.1.1

Identification and Authentication Controls	DoD	Air Force	Army	Navy	DLA	DFAS
There should be an audit trail of AIS use for each user	x			x	x	x
User shall have access to all information entitled	x					
Generic passwords are prohibited		x				
Established procedure available to allow users to change own passwords		x				
Audit accounts every 6 months to identify dormant IDs		x				
Safeguard internal security controls, passwords, and audit trails				x		
Randomly generated passwords are preferable				x		
Limit programmer access to the AIS				x		
Require users to log-off when leaving workstation			x			
Require an "idle screen lockout" after 3-5 minutes			x			
System auditing/monitoring to hold each individual with user access accountable for actions						x

DISA policies do not provide any additional identification and authentication controls.

National Institute of Standards and Technology Requirements. The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce, Technology Administration. In the Computer Security Act of 1987, Congress assigned responsibility to NIST for the preparation of standards and guidelines for the security of sensitive federal systems. The NIST handbook, dated October 1995, states that computer systems recognize people based on the authentication data the systems receive and lists passwords, tokens, and biometrics as the three most common means of authenticating a user's identity, which can be used alone or in combination. Passwords were previously discussed in this report.

Tokens. Objects that a user possesses for the purpose of identification and authentication are called tokens. Tokens are divided into two categories: memory tokens and smart tokens. Memory tokens store, but do not process information, for example, credit cards. A common application of memory

tokens for authentication to computer systems is the automatic teller machine card. A smart token expands the functionality of a memory token by incorporating one or more integrated circuits into the token itself, for example, a smart card. A smart card looks like a credit card, but incorporates an embedded microprocessor. Smart cards are defined by an International Standards Organization standard. Smart tokens that are not smart cards can look like calculators, keys, or other small portable objects.

Biometrics. Biometric authentication technologies use the unique characteristics (or attributes) of an individual to authenticate that person's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioral attributes (such as voice patterns and hand-written signatures). Biometric authentication technologies based upon these attributes have been developed for computer log-in applications.

DoD Component Use of NIST Requirements. DoD, OSD (AI-26), Navy, DLA, and DFAS did not discuss tokens or biometrics in their identification and authentication documents. The Army and Air Force discussed tokens and biometrics in their identification and authentication documents whereas DISA discussed tokens, but not biometrics.

Army. Specifically, the Army document states that biometric access control devices or smart cards provide practical alternatives for use in conjunction with, or in place of, password systems.

Air Force. The Air Force document states that possession-based identification and authentication systems require the user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain information coded in a form recognized by the host system. These systems reduce the threat from those attempting to guess or steal passwords, because the perpetrator must either fabricate a counterfeit token or steal a valid token. Examples of this technique include physical and electronic keys, challenge-response generators, smart cards and magnetic-strip cards or badges. The Air Force document also states that biometric-based identification and authentication systems rely on a unique physical characteristic to identify of a user. Common identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry.

DISA. The DISA document states that as a minimum, rules should include proper use of system privileges, sanctions regarding the unofficial use of DISA information technology, use of personally-owned software and hardware, connection to the internet, dial-in access, and protection of system authenticators, for example, smart cards and passwords.

Information Assurance Risk Factors

A combination of advances in information technology, interlinked and increasingly automated infrastructures, and the large volume of Y2K renovations have magnified overall information security risks for DoD.

Critical Infrastructures. Infrastructures have become increasingly automated and interlinked as a result of advances in information technology. These same advances have created new vulnerabilities to equipment failures, human error, and physical and cyber attacks. Presidential Decision Directive 63 requires the continuity and viability of critical infrastructures and the elimination of vulnerability to physical and cyber attacks on critical infrastructures. Critical infrastructures are those systems essential to the minimum operations of the economy and government.

Year 2000. The DoD year 2000 remediation efforts have provided opportunities to exploit existing vulnerabilities within information systems or networks. Such vulnerabilities have been used as a way to attack the information, information systems, and networks that comprise the Defense Information Infrastructure. To complement the external threat there is an insider threat. Year 2000 remediation efforts also provide employees and those associated with the year 2000 testing, evaluation, and renovation processes, opportunities to gain increased access to previously restricted systems.

Summary

The first line of defense against system intrusion is the ability to implement a uniform identification and authentication policy by DoD systems users, administrators, and managers. If the component policies vary in stringency, the weaker policies may well be an inherent casual factor that increases vulnerabilities. DoD lacks uniform requirements on identification and authentication controls. Consequently, DoD components have produced their own individual policies or operated under older procedures not consistent with or reflective of the current technological advances. These policies vary significantly and will continue to do so until DoD provides more specific guidance on uniform security requirements. DoD urgently requires additional policy guidance that specifically addresses the concerns expressed on identification and authentication.

Recommendations, Management Comments, and Audit Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

1. **Immediately provide specific interim policy guidance to establish minimum security requirements covering identification and authentication, and**

2. **Accelerate the reissuance of a governing DoD Directive.**

ASD(C³I) Comments. The ASD(C³I) concurred, stating that the Infrastructure and Information Assurance Directorate does not take exception to the recommendations.

Also, ASD(C³I) stated that AI-26 is only applicable to OSD and not to any of the components examined and it was not surprising that all of the 18 requirements in AI-26 are not fully covered by all other policies.

Additionally, ASD(C³I) stated that its draft identification and authentication policy did not provide detailed identification and authentication controls like those found in AI-26 because the approach taken in the policy is to allow the DoD Components discretion in implementation as long as they satisfy policy requirements for identification and authentication and interoperability.

Audit Response. The ASD(C³I) comments were generally responsive. For followup purposes, we need to know the estimated duties for completing the agreed-upon actions related to Recommendations 1 and 2.

The Senior Civilian Official, ASD(C³I) [now the ASD(C³I)], issued a memorandum on "Year 2000 and the Importance of Adherence to Department of Defense Information Security Policy," May 5, 1999, and asked that all personnel using DoD systems comply with the guidance in AI-26, Chapter 11, particularly Section 5.1.1. Rather than argue with the applicability of the citation in the May 5, 1999, memorandum, we used the content of AI-26 to measure the uniformity of requirements between security policies of various DoD Components. The audit results illustrate the wide range of disparity between the various policies and highlight the immediate need for a uniform set of DoD requirements for identification and authentication controls. If component policies vary in stringency, the weaker policies may well be an inherent causal factor that increases vulnerabilities. We are not advocating a policy on technological solutions, but rather a policy that outlines DoD expectations of minimum controls and protection. It is precisely because of the decentralized establishment of nonuniform policy requirements that an overall DoD information assurance management strategy continues to be inadequately implemented.

Appendix A. Audit Process

Scope

Review of Information Systems Security Policy. We compared current DoD and DoD Component policies addressing identification and authentication controls for information systems to those requirements appearing in OSD Administrative Instruction 26, Chapter 11, Section 5.1.1. We discussed the policies with the appropriate personnel as considered necessary.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from July through November 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD designated information assurance as a material management control weakness in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

General Accounting Office. General Accounting Office, Report No. AIMD-99-107, "DoD Information Security," August 1999, stated that users were granted computer resource accesses that exceeded what was required to carry out job responsibilities, including sensitive system privileges for which they had no need. The audit also found user accounts that had certain privileges but no authorization was available. Further, access authorization was poorly documented or undocumented and GAO estimated that on one system, more than 20,000 users were not authorized in writing. The audit found inadequate periodic review of user access privileges. Users were not required to change their passwords often enough, and in some cases, were never required to change passwords; and users were not

prevented from using easily guessed passwords. Those practices increased the risk that passwords would be guessed and systems would be compromised. DoD generally concurred with the report and the recommendations, noting that the report added credence to efforts to heighten awareness within the DoD community of the serious risks that accompany poor security practices in information systems.

Inspector General. Inspector General, DoD, Report No. 99-069, "Summary of Audit Results—DoD Information Assurance Challenges," January 22, 1999, identified 59 reports that discuss conditions related to access control weaknesses. The reports contain recommendations for access control improvements to various components, including the Army, Navy, Air Force, Defense Information Systems Agency, Defense Finance and Accounting Service, and Defense Investigative Service.

Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997, found that security safeguards and practices for DoD automated information systems were not adequate to protect classified and sensitive unclassified information from unauthorized access. Protection of automated information systems was inadequate because of ineffective implementation of the Defense-wide Information Systems Security Program, outdated policies and procedures, inadequate direction and oversight, and the lack of accountability for information systems security management controls.

Appendix B. Chronology of Actions Relating to Recommendations Made in Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems"

Date	Office of Primary Responsibility	Action	Promised Resolution Date
September 8, 1997	Acting ASD(C^3I)	Concurred with the two draft recommendations concerning revisions to DoD 5200.28 and stated that "the initial review of DoD Directive 5200.28 had been completed and would be available for formal review"	October 1997
September 25, 1997	DoD Inspector General Policy and Oversight Directorate	Final report published. Two recommendations addressed to revision of DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988	
March 4, 1998	Acting ASD(C^3I)	The Information Assurance Group completed review of the revised DoD Directive 5200.28. Comments and recommendations are being incorporated prior to submission of the document to the formal Department 106 coordination process.	March 31, 1998

Date	Office of Primary Responsibility	Action	Promised Resolution Date
October 2, 1998	Acting ASD(C^3I)	Provided copies of draft DoD Directive 8500.XX, "Information Assurance Program" and draft DoD Instruction 8500.XX, "Information Assurance Requirements" that will replace DoD Directive 5200.28. Formal review to begin before the end of calendar year.	December 31, 1998
June 16, 1999	ASD(C^3I)	DoD Chief Information Officer launched the Global Network Information Enterprise to develop fully coordinated information assurance policies. The DoD Chief Information Officer decided to delay the formal coordination of the Information Assurance directive and instruction and issue a policy memorandum instead. All Global Network Information Enterprise guidance and policy memoranda are to be completed by July 31, 1999. The Information Assurance Directorate will then convert the Information Assurance Memorandum to a separate DoD directive and instruction.	July 31, 1999

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense Command (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Chief Information Officer and Year 2000
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Security and Information Operations
Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Auditor General, Department of the Navy
Inspector General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  Technical Information Center, National Security and International Affairs Division
  Defense Information and Financial Management Systems, Accounting and Information Management Division

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Office Of The Assistant Secretary Of Defense Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

December 8,1999

MEMORANDUM FOR DIRECTOR FOR ACQUISITION MANAGEMENT,
OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on Identification and Authentication Policy
(Project No. 9AS-0048), November 17, 1999.

This memorandum is in response to your November 17, 1999 request for comments on the draft audit report on identification and authentication policy.

The Infrastructure and Information Assurance (I&IA) Directorate does not take exception to the finding at the top of page four of the draft report nor the recommendations on page fifteen. We do, however, offer the following comments and observations:

Comment: Your stated objectives were to "evaluate the adherence of system users to DoD information systems security policy, during and after year 2000 conversion efforts. Specifically,...using as criteria the requirements of Administrative Instruction (AI) 26-1, chapter 11, and Section 5.1.1."
Observation: As pointed out beginning at the bottom of page 1, AI 26-1 is only applicable to the Office of the Secretary of Defense (OSD) and not to any of the Components examined. That being true, the finding on page 7 that "None of the 18 requirements in AI 26-1 is fully covered by all other policies" is not surprising since there has never been a requirement for them to do so.

Comment: Page five of the draft report says that two drafts of ASD(C3I) guidance and policy for DoD IA were reviewed and that the "guidance did not provide detailed identification and authentication controls'
Observation: The draft IA policy does not provide detailed I&A controls like those found in AI 26-1 because the approach taken in the policy is to allow the Component's discretion in implementation as long as they satisfy policy requirements for IA and interoperability.. The draft policy does, however, require IA solutions at different levels of robustness, depending on the operational environment, and specifically addresses access controls in Enclosure #3.

My point of contact for this action is Mr. Donald L. Jones, telephone 703/614-6640, e-mail: donald.l.jones@osd.pentagon.mil.

Richard C. Schaeffer, Jr.
Director, Infrastructure and Information Assurance

Audit Team Members

The Acquisition Management Directorate Office of the Assistant Inspector General for Auditing, DoD, produced this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report, are listed below.

Thomas F. Gimble
Mary Lu Ugone
Dianna J. Pearson
Kathryn M. Truex
H. George Cherry
JoAnn Henderson
Jerry Hall
John J. Jenkins
Timothy A. Cole
Jamal Hall
Kevin W. Klein