July 29, 2002

Information System Security

User Authentication Protection at Central Design Activities (D-2002-135)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this evaluation report, visit the home page of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or 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.

Suggestions for Future Evaluations

To suggest ideas for or to request future 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 Evaluation Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

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

CDA	Central Design Activity
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

July 29, 2002

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

SUBJECT: Report on User Authentication Protection at Central Design Activities (Report No. D-2002-135)

We are providing this report for your review and comment. We considered management comments on a draft of this report when preparing the final report.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) was responsive to the intent of the recommendations. However we request that the Assistant Secretary provide additional comments by September 24, 2002, on when the proposed policy updates will be available to review.

We appreciate the courtesies extended to the staff. Questions on the evaluation should be directed to Mr. Kenneth Stavenjord at (703) 604-8952 (DSN 664-8952) (kstavenjord@dodig.osd.mil) or Mr. Peter Johnson at (703) 604-9601 (DSN 664-9601) (pjohnson@dodig.osd.mil). See Appendix C for the report distribution. The team members are listed inside the back cover.

David K Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2002-135 **July 29, 2002**
(Project No. D2000PT-0121.001)

User Authentication Protection at Central Design Activities

Executive Summary

Who Should Read This Report And Why? Officials and administrators who are responsible for DoD information systems should read this report. The report explains the extent of transmitting user passwords in plain text while accessing software development environments and the vulnerabilities associated with it.

Background. A Central Design Activity is defined as a designated organization within a Component that has responsibility for designing, converting, programming, testing, documenting, or subsequently maintaining computer operating or applications software for use at more than one location. We evaluated authentication protection at an Army, a Navy, and an Air Force Central Design Activity.

Central Design Activities use software development environments to develop and maintain the software for which they are responsible. A software development environment is an integrated suite of tools to aid the development of software in a particular programming language or for a particular application.

Logging on to the vast majority of computing systems, including software development environments, is protected by passwords. The person logging on must supply a user name plus the password associated with that user name. The system evaluates the password to verify the user’s identity claim. This process is called authentication. Password authentication mechanisms work if passwords are kept secret at all stages. During a previous evaluation, we confirmed at one central design activity that user names and passwords were transmitted in plain text to software development environments located at the Defense Information Systems Agency Defense Enterprise Computing Centers. Readily available software would permit an attacker to capture the transmitted user name and password for possible unauthorized accesses.

Results. User names and passwords were transmitted in plain text over unsecured networks on 15 of 26 software development environments at 3 Central Design Activities. As a result, the 15 software development environments have an increased risk of unauthorized access, unauthorized changes to DoD software, and loss of accountability. In addition, all unclassified DoD systems could be similarly affected. Additional policy was needed to ensure authentication information was protected during transmission over unsecured networks. See the Finding section for the detailed recommendation.

We had previously reported a similar problem in DoD Inspector General Report No. D-2000-058 "Identification and Authentication Policy", December 20, 1999. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) had not completed actions to issue policy to address the issue.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendation and stated that information assurance policy will be updated to require unclassified and classified systems protect authentication information during transmission by including it in the new information assurance DoD Instruction 8500.bb. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Evaluation Response. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments were responsive. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments by September 24, 2002, on when the proposed policy updates will be available to review for consistency with standards and guidance from the National Institute of Standards and Technology.

Table of Contents

Background

In Inspector General of the Department of Defense Report No. D-2001-046, "Evaluation of Information Assurance at Central Design Activities," February 7, 2001, we confirmed at a Defense Agency central design activity (CDA) that user names and passwords were transmitted in plain text over unsecured networks to software development environments. Readily available software would permit an attacker to capture the transmitted user name and password for possible unauthorized accesses. Because of concern about security issues we expanded our review to the Military Departments.

Central Design Activities. A CDA is defined as a designated organization, within a DoD Component, that has responsibility for designing, converting, programming, testing, documenting, or subsequently maintaining computer operating or applications software for use at more than one location. The Army, the Navy, and the Air Force have a total of 17 CDAs. See Appendix B for the CDA list.

For this evaluation, we visited the Software Engineering Center - Meade (Army) and the Fleet Material Support Office (Navy). We collected information assurance data from these CDAs and from the Materiel Systems Group (Air Force). Other DoD agencies have CDAs also. The Marine Corps, the Defense Finance and Accounting Service, the Director for Information and Technology, and the Defense Logistics Agency list CDA organizations.

Software Engineering Center - Meade. The Software Engineering Center – Meade in Fort Meade, Maryland, is a direct reporting unit of the Software Engineering Center, Communications and Electronics Command, U.S. Army Materiel Command. The Software Engineering Center – Meade has 76 employees and provides life-cycle support of software products.

Fleet Material Support Office. The Fleet Material Support Office in Mechanicsburg, Pennsylvania, is a major field organization of the Naval Supply Systems Command. The Fleet Material Support Office has more than 900 employees and provides information technology products and services to the Navy, DoD, and other Federal organizations. Their systems integrate supply, financial, maintenance, procurement, and other logistics functions through networks, telecommunications, and interrelated databases.

Materiel Systems Group. The Materiel Systems Group, Wright-Patterson Air Force Base, Ohio, is a direct reporting unit of the Electronic Systems Center, Air Force Materiel Command. The Materiel Systems Group supports the Air Force information goals through acquiring, developing, maintaining, reengineering, and providing technical services for information systems. The Materiel Systems Group has 576 employees and manages more than 160 of the Air Force Materiel Command's logistics information systems.

Software Development Environments. Central Design Activities use software development environments to develop and maintain the software for which they are responsible. A software development environment is an integrated suite of tools to aid the development of software in a particular programming language or for a particular application. A software development environment includes the facilities, networks, hardware, software, firmware, procedures, and documentation needed to perform software engineering. The software may include programming tools, documentation tools, debugging tools, test tools, source code management tools, and database management systems.

System User Authentication. Logging on to the vast majority of information systems, including software development environments, is protected by passwords. The person logging on must supply a user name plus a password associated with that user name. The system evaluates the password to verify the user's identity claim. This process is called authentication. Password authentication works when the passwords are kept secret at all stages. Secrecy can be lost when passwords are entered, transmitted, and stored. When passwords are transmitted in plain text, they are vulnerable to electronic eavesdropping.

Prior Audit Coverage. Inspector General of the Department of Defense Report No. D-2000-058, "Identification and Authentication Policy," December 20, 1999, references the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum on "Year 2000 and the Importance of Adherence to Department of Defense Information Security Policy," May 5, 1999. The memorandum recommended that all personnel using DoD systems comply with the guidance in AI-26, chapter 11, and particularly section 5.1.1. We used the referenced AI-26 guidance to determine whether security policies of various DoD Components were uniform. Of the 18 AI-26 identification and authentication requirements evaluated, none addressed the vulnerability of transmitting passwords in plain text or set requirements for password protection while being transmitted for logon. The results illustrated wide discrepancies between the various policies, which highlighted the need for uniform DoD requirements for identification and authentication controls. The report recommended the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) develop interim guidance to establish minimum security requirements covering identification and authentication, and accelerate the reissuance of a governing DoD directive. The extended time needed to coordinate DoD guidance to address the issues has delayed implementation of the recommendations.

Objective

The objective of this evaluation was to assess the extent of the transmission of software development environment user names and passwords in plain text and how this vulnerability was addressed.

Authentication Vulnerability

At the three CDAs we evaluated, the user names and passwords were transmitted over unsecured networks to their software development environment hosts. The CDAs reported that in 15 of 26 software development environments, the user passwords were transmitted in plain text. Passwords were transmitted in plain text because DoD information assurance policy did not require protection of authentication information during transmission to unclassified systems and did not require National Institute of Standards and Technology security guidance to be followed, as required by Office of Management and Budget Circular No. A-130. As a result, the 15 software development environments have an increased risk of unauthorized access, unauthorized changes to DoD software, and loss of accountability. In addition, because of the lack of explicit DoD policy on this matter, all unclassified DoD systems could be similarly affected.

Vulnerability, Threat, and Safeguard

The concepts of vulnerability, threat, and safeguard make up a framework for thinking about computer security. Vulnerability is a weakness of a system that would allow system security to be violated. A threat is a circumstance or event that could cause harm by violating security. A threat often exploits a vulnerability. A safeguard is any technique, procedure, or other measure that reduces vulnerability. Some threats aim at safeguards such as passwords.

Reliable authentication mechanisms are critical to the security of any automated information system. In the past, it was relatively easy to protect computer systems because they were typically installed in centralized computing facilities. Because the terminals used to access the computer were usually in the same building, only those persons having physical access to the building had use of the terminals. However, this level of physical control is no longer viable because of the proliferation of networked computer systems. Networking makes it more difficult to identify system users and increases opportunities for unauthorized parties to eavesdrop on legitimate user and remote host computer sessions. User passwords were sometimes transmitted through the network in plain text form. If an attacker were able to eavesdrop on the user's session, the attacker could record the user's password or other critical authentication data. The attacker could pose as a valid user by logging on the remote host using the recorded authentication data.

Monitoring network information is called "sniffing." Software is readily available for monitoring network traffic, primarily for the purpose of network performance management and problem diagnosis. The same software is often quite effective for capturing passwords during network transmissions. Unauthorized sniffers can be extremely dangerous to network security because they are virtually impossible to detect and can be inserted almost anywhere in the network. Attempts to use firewalls to solve these security problems assume that "the bad guys" are on the outside, which is often a wrong assumption.

Insiders carry out most of the seriously damaging incidents of computer crime. Some systems apply a cryptographic algorithm to scramble (encrypt) the password before transmission so that the plain text password is not exposed. However, an attacker could record the encrypted password and use it to gain access to the host computer. In either case, the host computer cannot distinguish between the attacker and a valid user, and access is granted.

One-time password technology uses passwords that, if intercepted, cannot be used for future access. One approach to one-time passwords is to have the remote host provide challenge information, such as a word for one-time use, when an authorized user connects. The challenge information and user password are plugged into an algorithm, which generates the response that the remote host verifies. With this approach, the password is never transmitted over the network, nor is the challenge used twice. Some approaches use passwords combined with time slots and a time synchronized host. Others use a card system with stored numbers and the remote host uses a matching list of numbers.

User Name and Password Transmissions

At the three CDAs we evaluated, the user names and passwords were transmitted over unsecured networks to their software development environment hosts. The CDAs reported that in 15 of 26 software development environments, the user passwords were transmitted in plain text. Of the 11 software development environments with protected logon passwords, 10 used encryption features provided by the commercial software tools in their software development environments. One development project used a separate and dedicated network to mitigate the plain text password risk sufficiently and was considered adequately protected. Other risk reduction approaches, such as switched networks and firewalls, were not sufficient to protect the plain text passwords from an insider attack. One-time passwords from a smart card, token, or encrypted challenge/response dialog offered increased protection because the transmitted password was good for just one use. These solutions were only granted to privileged users such as system programmers, network administrators, and database administrators.

Transmitting logon passwords in plain text to the host computer was not unique to software development environments. The DISA Field Security Office and the Defense Enterprise Computing Center at Mechanicsburg observed that most system user logon passwords were transmitted in plain text.

The National Bureau of Standards, now known as the National Institute of Standards and Technology (NIST), identified the vulnerability of passwords transmitted in plain text over unsecured networks in the Federal Information Processing Standards (FIPS) Publication 83, "Guideline on User Authentication Techniques for Computer Network Access Control," September 1980. They warned of wiretapping and electronic eavesdropping and recommended a process that encrypted passwords differently each time the encryption process was used. FIPS Publication 190, "Guideline for the Use of Advanced Authentication Technology Alternatives," September 1994 and NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST

Handbook," October 1995 both contain extensive information on the password transmission vulnerability and possible safeguards. The threat was described as electronic monitoring and the safeguards were updated to include authentication tokens and biometrics. Since 1980, the message has been that organizations should protect authentication data transmitted over public or unsecured networks.

Information Assurance Requirements and Guidance

Federal Policy. Office of Management and Budget (OMB) Circular No. A-130, February 8, 1996, establishes policy for the management of Federal information resources. Circular No. A-130 states that agencies will protect Government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to, or modification of, information. Circular No. A-130 tasks the Secretary of Commerce to develop and issue Federal Information Processing Standards (FIPS) and guidelines for Government information technology. Circular No. A-130 requires agencies to use Federal Information Processing Standards where appropriate or required. Appendix III of Circular No. A-130, "Security of Federal Automated Information Resources," states that agencies shall implement and maintain a program to assure that adequate security is provided for all agency information in general support systems and major applications. Each agency's program shall implement policies, standards, and procedures that are consistent with Government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, and General Services Administration, and the Office of Personnel Management. Appendix III further states that agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. The November 30, 2000, update to Circular No. A-130 requires the agency annual Information Technology Capital Plan to explain any planned or actual variance from NIST security guidance.

DoD Policy. The primary DoD information assurance policy is DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 1988. DoD Directive 5200.28 states that unclassified information in automated information systems shall be safeguarded against tampering, loss, and destruction, and shall be available when needed. DoD Directive 5200.28 references OMB Circular No. A-130 for suggested safeguards for unclassified information but includes no references to Federal Information Processing Standards or requirements to implement NIST security guidance. The minimum safeguards for automated information systems that process classified and sensitive unclassified information require the positive identification of each user before authorizing access to the system. The policy does not establish a baseline for protection of authentication information when used to logon to hosts over unsecured networks.

Air Force Manual 33-223, "Identification and Authentication," June 1998 was the only Component policy to address the transmission of passwords. The manual states:

> Protect passwords during transmission at the same level required for the system or data the password is protecting. Passwords are typically sent from a terminal to the system by a communication line. Unless the line is physically protected or encrypted, the password is vulnerable to disclosure by wiretapping and/or sniffers. Prevent this vulnerability by electronic protection or password encryption. Increasing the password length and changing it more often can mitigate this vulnerability.

The policy discusses the transmission vulnerability but is not clear about protecting passwords.

The DoD Chief Information Officer Guidance and Policy Memorandum 6-8510, "Department of Defense Global Information Grid Information Assurance," June 2000 sets user access to mission support or administrative data at the basic robustness level. Basic robustness is equivalent to good commercial practice and is the lowest level of security services described in Memorandum 6-8510. The basic robustness level of authenticated access control includes digital signature (public key encryptography based), challenge/response identification and authentication, or preplaced keying material. Although the memorandum has expired, it is still being used and it shows the intended direction for DoD information assurance policy.

Unprotected Transmission of Authentication Information

The GAO/AIMD-98-274 report, "Financial Management, Improvements Needed in Air Force Vendor Payment Systems and Controls," September 1998 identified systems that are vulnerable to penetration by unauthorized internal users because vendor payment system passwords and user names are transmitted across the local network and communication links in plain text. Readily available software would permit any user to read vendor payment system passwords and user names. Thus, a clerk could obtain the passwords and user names of employees with higher access and use this information to enter the vendor payment system and perform all payment processing functions. Technological controls could be used to improve user authentication procedures, such as a smart card.

The June 7, 2001, Security Wire Digest reports that an attacker gained access to the server of a commercial software development organization and accessed their source code repositories. Security specialists and administrators determined the extent of the intrusion, repaired the damage, and brought the server back online. There was no evidence that any code was affected. The attacker had subverted the client code at a remote site and captured the logon name and password of a user who logged onto the server. Once the attacker was accepted as an authorized user, the attacker used a weakness of the server system to gain root privileges. At that point, the attacker modified the client and server systems to record user names and passwords. Some insider knowledge may have helped the attacker select the remote site and modify the systems.

It has long been recognized that the greatest harm to systems and their data has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability. Accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. If an attacker impersonates an authorized user, accountability will identify the authorized user, not the attacker. The attacker could make unauthorized changes to the system or the data.

Summary

When user names and passwords are transmitted over unsecured networks in plain text, they are vulnerable to electronic eavesdropping. This vulnerability has been a known security risk for years and solutions are available. However, 15 of 26 software development environments we reviewed continue to operate with this vulnerability. NIST security standards address this vulnerability, and the OMB Circular No. A-130 requires the use of these standards in Federal agency information assurance programs. However, DoD policies do not reference or require compliance with NIST security standards and do not require protection of the passwords when transmitted to unclassified hosts. The unprotected user name and password can be captured and used to impersonate the authorized user for unauthorized access to the system, and could result in unauthorized changes to the system or the data. In addition, because of the lack of explicit DoD policy on this matter, all unclassified DoD systems could be similarly affected.

Recommendation, Management Comments, and Evaluation Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) update DoD information assurance policy to require unclassified systems to protect authentication information during transmission over unsecured networks and to use security products and techniques that are consistent with standards and guidance from the National Institute of Standards and Technology.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C^3I]) concurred with the recommendation and stated that information assurance policy will be updated in the new DoD Instruction 8500.bb by including the requirement for unclassified as well as classified systems to protect authentication information during transmission. Specifically, the new DoD Instruction 8500.bb will incorporate words to protect authentication information during transmission "both as a responsibility of users and in the appropriate controls relating to the treatment of individual identification and authentication."

Evaluation Response. The ASD(C^3I) comments are responsive. In response to the final report, we request that the ASD(C^3I) provide dates when the proposed policy updates will be available to review for consistency with standards and guidance from the National Institute of Standards and Technology.

Appendix A. Scope and Methodology

Work Performed. We evaluated authentication protection in 26 software development environments at 3 Central Design Activities. We developed two questionnaires, one to be used for each software development environment and the other to determine the security policies and procedures in effect for the organizations. We collected answers to the policy questionnaire from all organizations that we contacted during this evaluation. The software development environment questionnaires were collected from the Central Design Activities that we contacted. We also reviewed relevant policy at the Federal, DoD, and Services levels.

We analyzed the questionnaire results, documents, and referenced web sites. We reviewed prior audit and evaluation reports for related coverage.

Limitations to Scope. We did not review the management control program related to the evaluation objective because DoD has recognized Information Assurance as a material management control weakness area since the FY 1999 Annual Statement of Assurance.

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.

Use of Computer-Processed Data. We did not use computer-processed data to perform this evaluation.

Evaluation Type, Dates, and Standards. We performed this evaluation from September 2000 through December 2001 in accordance with standards implemented by the Inspector General, DoD. Our scope was limited in that we did not include tests of management controls.

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

Prior Coverage

During the past 5 years, the General Accounting Office and the Inspector General of the Department of Defense issued reports that discussed the vulnerability of transmitted passwords and information assurance policy.

General Accounting Office

GAO Report No. GAO/AIMD-98-274, “Financial Management, Improvements Needed in Air Force Vendor Payment Systems and Controls,” September 1998

Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2000-124, “Information Assurance Challenges—A Summary of Audit Results Reported December 1, 1998, through March 31, 2000,” May 15, 2000

IG DoD Report No. D-2000-058, “Identification and Authentication Policy”, December 20, 1999

IG DoD Report No. 99-069, “Summary of Audit Results—DoD Information Assurance Challenges,” January 22, 1999

Unrestricted Inspector General of the Department of Defense reports can be accessed over the Internet at http://www.dodig.osd.mil/audit/reports.

Appendix B. Military Department Central Design Activities

Central Design Activities

For the purpose of this evaluation, a Central Design Activity (CDA) is defined as a designated organization, within a DoD Component, that has responsibility for designing, converting, programming, testing, documenting, or subsequently maintaining computer operating or applications software for use at more than one location.

Although each Military Department's definition of a CDA may vary slightly from the definition above, they each identified their CDAs (see table below) and noted that they had other software development groups that were not CDAs. Those other software development groups are not considered CDAs because they support software only for the business area organization they belong to, as opposed to more than one location as our definition of CDAs requires.

Military Department Central Design Activities

Army
Army Total Personnel Command
Industrial Logistics Systems Center
Logistics Systems Support Center
Software Engineering Center – Belvoir
Software Engineering Center - Lee
Software Engineering Center – Meade

Navy
Bureau of Naval Personnel
Fleet Material Support Office
Naval Aviation Depot Operations Center
Naval Computer and Telecommunications Area Master Station, Atlantic
Naval Computer and Telecommunications Station, Jacksonville
Naval Computer and Telecommunications Station, Pensacola
Naval Computer and Telecommunications Station, Washington
Naval Education and Training Professional Development and Technology Center
Naval Reserve Information Systems Office

Air Force
Materiel Systems Group
Standard Systems Group

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
  Deputy Assistant Secretary of Defense, Security and Information Operations
    Director, Infrastructure and Information Assurance
    Director, Policy Integration and Operations

Joint Staff

Director, Joint Staff
  Director, Operations
  Director, Command, Control, Communications, and Computers

Department of the Army

Commanding General, Army Communications and Electronics Command
  Commander, Software Engineering Center - Meade
Auditor General, Department of the Army

Department of the Navy

Commander, Naval Supply Systems Command
  Commanding Officer, Fleet Material Support Office
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Commander, Air Force Materiel Command
    Executive Director, Materiel Systems Group
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
    Commander, Defense Information Systems Agency Western Hemisphere

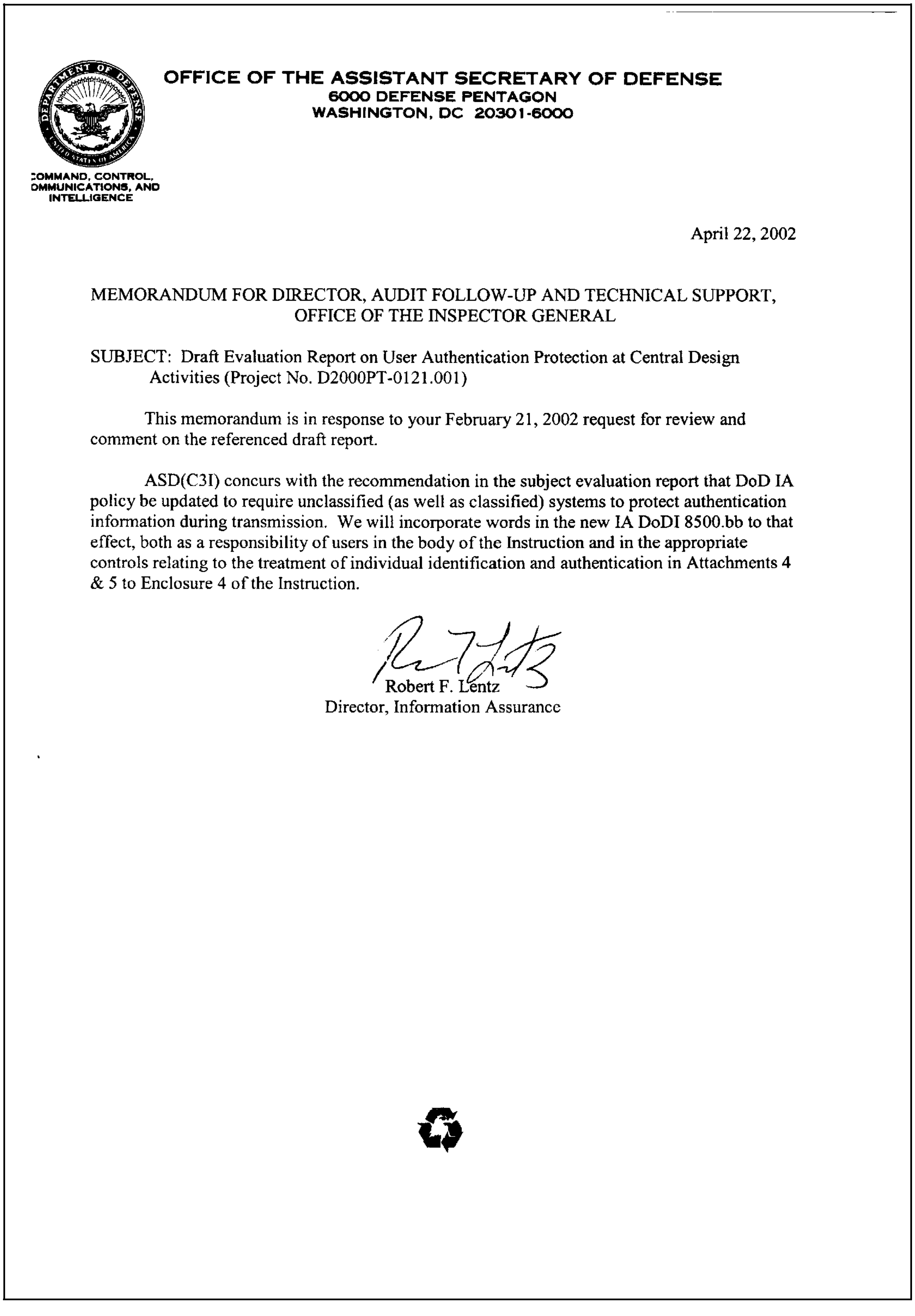
Non-Defense Federal Organizations

Office of Management and Budget

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 Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



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

COMMAND, CONTROL,
OMMUNICATIONS, AND
INTELLIGENCE

April 22, 2002

MEMORANDUM FOR DIRECTOR, AUDIT FOLLOW-UP AND TECHNICAL SUPPORT,
OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Evaluation Report on User Authentication Protection at Central Design Activities (Project No. D2000PT-0121.001)

This memorandum is in response to your February 21, 2002 request for review and comment on the referenced draft report.

ASD(C3I) concurs with the recommendation in the subject evaluation report that DoD IA policy be updated to require unclassified (as well as classified) systems to protect authentication information during transmission. We will incorporate words in the new IA DoDI 8500.bb to that effect, both as a responsibility of users in the body of the Instruction and in the appropriate controls relating to the treatment of individual identification and authentication in Attachments 4 & 5 to Enclosure 4 of the Instruction.

Robert F. Lentz
Director, Information Assurance

TEAM MEMBERS

The Audit Followup and Technical Support Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

David A. Brinkman
Kenneth H. Stavenjord
Peter C. Johnson