udit

eport

FOREIGN NATIONAL ACCESS TO
AUTOMATED INFORMATION SYSTEMS

Report No. D-2000-130 May 26, 2000

Office of the Inspector General
Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Additional Copies

To obtain additional copies of this audit 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.

Suggestions for Future Audits

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 Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

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

AIS	Automated Information System
DDL	Delegation of Disclosure Authority Letter
LAN	Local Area Network
NAVAIR	Naval Air Systems Command
NAWCAD	Naval Air Warfare Center, Aircraft Division
NAWCWD	Naval Air Warfare Center, Weapons Division

Office of the Inspector General, DoD

Report No. D-2000-130 **May 26, 2000**
(Project No. 9LG-5030.01)

Foreign National Access to Automated Information Systems

Executive Summary

Introduction. Public Law 106-65, National Defense Authorization Act for Fiscal Year 2000, section 1402, "Annual Report on Transfer of Militarily Sensitive Technologies to Countries and Entities of Concern," requires an annual interagency review on the transfer of militarily sensitive technology to countries and entities of concern.

Objectives. The overall audit objective was to evaluate the adequacy of DoD policies and procedures to prevent the transfer of technologies and technical information with potential military application to countries and entities of concern. Project No. 9LG-5030 "Export Licensing at DoD Research Facilities," February 8, 2000, addresses the DoD portion of the required FY 2000 export licensing interagency review at DoD research facilities. For this report, we evaluated whether automated information system access controls and physical security controls for foreign national visitors were adequate at research facilities owned or sponsored by DoD. We also reviewed the management control program as it related to our objective.

Results. The Army and the Navy did not have adequate procedures for authorizing and controlling access by foreign nationals to information available on automated information systems and local area networks. In addition, the Navy did not have adequate procedures for identifying foreign nationals in e-mail communications. However, the Air Force had adequate procedures for automated information system and local area network access as well as e-mail communications by foreign nationals. As a result, at least 23 foreign nationals at two Army research facilities visited and 103 foreign nationals at 5 of the 6 Navy systems commands and research facilities contacted had unrestricted access to automated information systems and local area networks. In addition, the e-mail correspondence of at least 53 foreign nationals at 4 of the 6 Navy facilities contacted had no distinguishing identifiers. The foreign nationals could gain unauthorized access to militarily sensitive technologies and other controlled unclassified information that may be available through the unrestricted use of automated information systems and local area networks at Army and Navy facilities or through e-mail communications at Navy facilities. See the Finding section for details on the audit results and Appendix A for details on the management control program. See Appendix C for other matters of interest.

Summary of Recommendations. We recommend that the Army and the Navy revise applicable regulations to ensure foreign national visitors cannot gain access to militarily sensitive technologies and other controlled unclassified information that is available on local area networks or through electronic communications with others outside of the local area network.

Management Comments. The Office of the Director of Information Systems for Command, Control, Communications, and Computers concurred with the finding and recommendation, stating the recommended changes are incorporated in Army Regulation 25-XX, scheduled to replace Army Regulation 380-19 in October 2000.

Audit Response. The Army response was not fully responsive. Office of the Director of Information Systems for Command, Control, Communications, and Computers comments concerning Army Regulation 380-19 were responsive. However, that office does not have purview over Army Regulation 380-10 and, therefore, could not respond concerning changes to that regulation. We ask that the Army Deputy Chief of Staff for Intelligence provide comments on the final report concerning Army Regulation 380-10 by June 26, 2000.

We did not receive comments from the Navy concerning changes to its instructions. We ask that the Navy Chief Information Officer; the Office of the Chief of Naval Operations; and the Director, Navy International Programs Office, provide comments on the final report by June 26, 2000.

See the Finding section for a discussion of management comments and the Management Comments section for the complete text.

Table of Contents

Background

Public Law 106-65, National Defense Authorization Act for Fiscal Year 2000, section 1402, "Annual Report on Transfer of Militarily Sensitive Technologies to Countries and Entities of Concern," October 5, 1999, requires that the Departments of Commerce, Defense, Energy, and State, in consultation with the Director of the Central Intelligence Agency and the Director of the Federal Bureau of Investigation, conduct reviews of the transfer of militarily sensitive technologies to countries and entities of concern. Project No. 9LG-5030, "Export Licensing at DoD Research Facilities," February 8, 2000, addresses the DoD portion of the required FY 2000 export licensing interagency review at DoD research facilities. This report addresses foreign national access to automated information systems (AISs) and physical security controls. During FY 1998 and FY 1999, the six sites included in our review had 11,542 approved foreign visitors.

The release of technology to foreign nationals working in or visiting DoD facilities requires some type of protection or control and must meet the requirements of DoD Regulation 5200.1-R, "Information Security Program," January 1997; DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988; DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992; and DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals," August 12, 1998.

DoD Regulation 5200.1-R. DoD Regulation 5200.1-R states that "[t]here is information, other than classified information, that has been determined to require some type of protection or control. This information is generally known as controlled unclassified information." Appendix C of the regulation, "Controlled Unclassified Information," states that the term includes "For Official Use Only, Sensitive But Unclassified, DoD Unclassified Controlled Nuclear Information, Sensitive Information as defined by the Computer Security Act of 1987," and information contained in limited distribution technical documents.

DoD Directive 5200.28. DoD Directive 5200.28 provides DoD policy for safeguarding classified, sensitive unclassified, and unclassified information processed in AISs and networks that include AISs.

DoD Directive 5230.11. DoD Directive 5230.11 implements National Disclosure Policy-1[1] and updates policy, responsibilities, and procedures governing proposed disclosures of classified military information to foreign governments and international organizations.

[1] Promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance required by departments and agencies having occasion to release classified military information to foreign governments and international organizations.

DoD Directive 5230.20. DoD Directive 5230.20 establishes and describes the process for visit assignments of foreign nationals to DoD Components or to contractor facilities over which the DoD Components have security responsibility.

Objectives

The overall audit objective was to evaluate the adequacy of DoD policies and procedures to prevent the transfer of technologies and technical information with potential military application to countries and entities of concern. Specifically, we evaluated whether AIS access controls and physical security controls for foreign national visitors were adequate at research facilities owned or sponsored by DoD. We also reviewed the management control program as it related to our objective. See Appendix A for a discussion of the audit scope and methodology and our review of the management control program. See Appendix B for prior coverage related to the objectives. See Appendix C for a discussion on physical security controls for foreign national visitors.

Information Systems Security

The Army and the Navy did not have adequate procedures for authorizing and controlling access by foreign nationals to information available on AISs and local area networks (LANs). In addition, the Navy did not have adequate procedures for identifying foreign nationals in e-mail communications. However, the Air Force had adequate procedures for AIS and LAN access as well as e-mail communications by foreign nationals. Adequate procedures were not in place because the Army and the Navy had not implemented the DoD requirements concerning AIS and LAN access by foreign nationals. The Navy had not implemented DoD requirements concerning e-mail identification. As a result, at least 23 foreign nationals at two Army research facilities visited and 103 foreign nationals at 5 of the 6 Navy systems commands and research facilities contacted had unrestricted access to AISs and LANs. In addition, the e-mail correspondence of at least 53 foreign nationals at 4 of the 6 Navy facilities contacted had no distinguishing identifiers. The foreign nationals could gain unauthorized access to militarily sensitive technologies and other controlled unclassified information that may be available through the unrestricted use of AISs and LANs at Army and Navy facilities or through e-mail communications at Navy facilities.

DoD Requirements

DoD Approval Authority for Foreign National Access to AISs and Networks. DoD Directive 5200.28 states that "access by foreign nationals to a Government-owned or Government-managed AIS may be authorized only by the DoD-Component Head." The directive also 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." AISs are used to access information on LANs. The directive also requires that an AIS information systems security officer be given the authority to enforce security policies and safeguards for all users.

DoD Disclosure Requirements. DoD Directive 5230.20 establishes the International Visits Program. Under the program, foreign nationals may be assigned as foreign liaison officers or as civilian employees who are authorized to act as official representatives of their government. Foreign exchange personnel may also be assigned to a DoD Component in accordance with the terms of an exchange agreement, to perform prescribed duties for the DoD Component as a part of the Defense Personnel Exchange Program.

Cooperative Program Personnel are foreign nationals assigned to a multinational program office that is hosted by a DoD Component in accordance with the terms of a Cooperative Program International Agreement.

DoD Directive 5230.20 states that designated disclosure authorities[2] issue delegation of disclosure authority letters (DDLs) that describe classification levels, categories, scope, and limitations to information that may be disclosed to specific foreign national visitors. Foreign disclosure officers and contact officers are responsible for ensuring that foreign nationals are to have access to only that classified and controlled unclassified information that has been authorized for release to the foreign national's government and that is necessary to fulfill the terms of their assignments.

The directive also states that foreign nationals are not to be permitted access to AISs unless the systems have been sanitized or configured to ensure that the foreign national's access to classified and controlled unclassified information is limited to that which has been authorized for release to his or her government. The directive also requires foreign nationals to identify themselves when dealing with others through oral, written, and electronic communications, such as e-mail, but does not provide an example or require a DoD-wide standard e-mail address format.

Army Implementation of DoD Requirements

The Army did not have adequate procedures for assigning LAN accounts to foreign nationals because the DoD requirement to control foreign visitor access to information on LANs had not been implemented by the Army. However, the Army had implemented the DoD requirement for control of foreign nationals through foreign identification in e-mail addresses. As a result, the Army had no assurance that controls over at least 23 foreign national visitors were adequate to protect against the unauthorized access to militarily sensitive technologies and information by foreign national visitors having LAN access.

Army Technology Security Policy. Army policy on the disclosure of Army technical information is described in Army Regulation 380-10, "Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives," December 30, 1994. The regulation provides policy on disclosure criteria, conditions, and limitations for release of Army technical information to foreign nationals. Specifically, the regulation states that foreign liaison and exchange personnel "may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is releasable to their government." A revised regulation, which updates areas other than access by foreign national visitors, was pending approval as of March 3, 2000.

[2] A designated disclosure authority is an official with the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk.

Army Information Security Policy. Although not specifically addressing foreign national visitors, the Army implementation of DoD Directive 5200.28 requirements for access to information on AISs, including networks, is described in Army Regulation 380-19, "Information Systems Security," February 27, 1998. The regulation states: "Each AIS will have an associated access control policy that will include features or procedures to enforce the access control measures required for the information within the AIS. The identity of each authorized user will be established positively before granting access." The regulation also states that designated disclosure authorities are responsible for the overall security of each AIS and that information system security officers are responsible for ensuring that users have the appropriate security clearances, authorizations, and "need-to-know." In addition, the regulation states that the minimum AIS security requirements are to be based on the maximum clearance of the least cleared user.

Army Policy on Foreign National Access to LANs. Army interim policy on foreign national access to LANs is included in a memorandum from the Director, Counterintelligence and Human Intelligence, Office of the Deputy Chief of Staff for Intelligence, "Foreign Representative Access to Army Computers and Computer Networks Interim Policy," August 10, 1998. The interim policy clarifies "Army policy on foreign [national] access to computers and computer networks, and [brings] the Army more into line with other Service, Joint Staff and DoD Agency policies." The interim policy references DoD Directive 5200.28 and addresses foreign national network access for classified and controlled unclassified information. The interim policy states that access may only be granted to LANs at Army sites if the network administrator is able "to absolutely verify that all the information on a LAN is authorized for release to the foreign nationals" working at the site. The interim policy specifies that "the appropriate accreditation authority" must be notified before access is provided to foreign nationals. The interim policy also states that when a foreign national is given access to an unclassified LAN, administrators are to place an identifying "caveat or marker on all outgoing e-mails." Such identification is intended to make all e-mail recipients aware that the sender may not have a "need to know" for some controlled unclassified information. Army Regulations 380-10 and 380-19 needed to be revised to include those requirements.

Army Materiel Command Letter of Instruction on Computer Support to Foreign Nationals. The Army Materiel Command implemented the interim policy in a letter of instruction to its Major and Subordinate Commands. The letter of instruction, "Intelligence Support to AMC [Army Materiel Command] International Agreements/Foreign Representation," December 17, 1999, provides guidance based on the rewritten Army Regulation 380-10 and experience acquired since publishing the former Army Materiel Command letter of instruction (same title), November 6, 1998. The December letter states that the host agency foreign disclosure officer is to receive, from the information system security officer or the information systems security manager, a written certification that assures that adequate safeguards are in place to prevent unauthorized foreign national access to information not specifically outlined in applicable DDLs.

Army Action. The Army Armament Research, Development and Engineering Center, Picatinny Arsenal, New Jersey, and the Army Communications-Electronics Command, Fort Monmouth, New Jersey, had not implemented DoD guidance and guidance in the Army Materiel Command's letter of instruction. At neither installation had the information system security officer or information systems security manager provided the foreign disclosure officer written certification that only the authorized computer access, identified in the proposed DDL of the potential foreign national visitor, was accessible by the foreign national. The foreign disclosure officers at Picatinny Arsenal and at Fort Monmouth had approved computer access for foreign representatives. Neither foreign disclosure officer had received required written assurance from the information system security officer or the information systems security manager that the computer system used by the foreign national visitor had been tested and certified that it could not access information and areas on the LAN that were not authorized. As a result, the Army Armament Research, Development and Engineering Center and the Army Communications-Electronics Command had no assurance that 23 foreign national visitors who had computer access at the time of our visit were not able to obtain militarily sensitive technologies and technical information for which they were not authorized.

Picatinny Arsenal and Fort Monmouth had implemented the Army requirement to identify foreign national visitors through their e-mail address. However, the implementation was not standard. At the Army Armament Research, Development and Engineering Center, foreign national visitors' e-mail addresses identified the country and the government project or program that the foreign national visitor was working under. At the Army Communications-Electronics Command, foreign national visitors' e-mail addresses identified the foreign country that they were from.

Navy Implementation of DoD Requirements

The Navy did not have adequate procedures for assigning LAN accounts to foreign nationals because the Navy had not implemented the DoD requirement to control foreign national access to information on LANs. At least 103 foreign national visitors at 5 of the 6 Navy systems commands and product centers, where research facilities were located, had unrestricted LAN access. In addition, the e-mail correspondence of at least 53 foreign nationals at 4 of the 6 Navy facilities contacted had no distinguishing identifiers because the Navy had not published the requirements contained in DoD Directive 5230.20.

Navy Organization. The Naval Air Systems Command (NAVAIR), the Naval Sea Systems Command, the Naval Supply Systems Command, and the Space and Naval Warfare Systems Command are second echelon systems commands that report to the Chief of Naval Operations. Those commands are primarily responsible for the acquisition, development, modernization, and support of weapon systems. The research, development, test, and evaluation of weapon systems is performed either at contractor facilities or at Navy-owned facilities

under third echelon commands. The third echelon commands are sometimes referred to as product centers. Approximately 80 percent of the foreign national visitors at the systems commands and product centers are assigned to NAVAIR, the Naval Sea Systems Command, and the Space and Naval Warfare Systems Command.

Navy Technology Security Policy. Secretary of the Navy Instruction 5510.34, "Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations," November 4, 1993, has not been updated to reflect DoD Directive 5230.20 requirements concerning foreign national access to LANs and identification of foreign nationals. According to the Acting Branch Head, Foreign Visits and Disclosure Branch, Navy International Programs Office, a revised instruction was being drafted that will include a reference to those requirements. However, security officials at NAVAIR and the Space and Naval Warfare Systems Command have attempted to implement those requirements and experienced problems. The Navy needs to provide specific guidance on how commands are to implement the requirements of DoD Directive 5230.20, not just reference the requirements.

Secretary of the Navy Instruction 5510.34 generally addresses the disclosure of controlled unclassified information to foreign national visitors. However, the instruction focuses on the access privileges of foreign exchange personnel. The instruction states that foreign exchange personnel are to be "fully integrated into the host command," and, although subject to restrictions on access to classified information, they are generally to be treated as members of the command. That guidance to fully integrate foreign exchange personnel into the host commands to which they are assigned is one reason why unrestricted LAN accounts were assigned to foreign nationals at 5 of the 6 Navy command headquarters and product centers contacted. However, the instruction also states that "disclosure of unclassified material with a military or space application or information marked 'For Official Use Only' must be sent to the appropriate foreign disclosure official for final release determination."

The Director of Security, Navy Information Network Program Office, stated that his office had not published any guidance on limiting LAN access or identifying foreign national visitors in electronic communications. The Director stated that guidance on the requirement for support services contractor personnel to change their e-mail addresses by adding "Contractor" after their names was published; however, guidance on the e-mail addresses of foreign nationals had not been published.

Navy Information Security Policy. Secretary of the Navy Instruction 5239.3, "Department of the Navy Information Systems Security Program," July 1995, states that the Chief of Naval Operations has overall responsibility for the Navy Information Systems Security Program. The instruction defines information systems security as "[t]he protection of information systems against unauthorized access to or modification of information . . . or the provision of service to unauthorized users." The provisions of the instruction were implemented by Chief of Naval Operations Instruction 5239.1B, "Navy Information Assurance Program," November 1999. Secretary of the Navy

Instruction 5510.36, "Department of the Navy Information Security Program Regulation," March 17, 1999, states that the Navy Chief Information Officer is responsible for issuing policies and guidance for the Navy Information Systems Security Program. According to an official responsible for network and data security policy in the Office of the Director, Space Information Warfare Command and Control, Office of the Chief of Naval Operations, the DoD Directive 5200.28 requirement concerning approval for access by foreign nationals to a LAN was not specifically addressed in Navy instructions. The official also stated that the Navy had not issued guidance on how to implement the requirements of DoD Directive 5230.20 on limiting LAN access and e-mail identification of foreign national visitors.

Navy Actions. We visited NAVAIR headquarters and two NAVAIR product centers to determine how LAN access by foreign national visitors was controlled. The two product centers we visited were the Naval Air Warfare Center, Aircraft Division (NAWCAD), located at Patuxent River, Maryland, and the Naval Air Warfare Center, Weapons Division (NAWCWD), located at China Lake, California. We also contacted security officials at three other Navy organizations where cooperative program personnel, foreign exchange personnel, or foreign liaison officers were assigned to determine whether there were controls over LAN access by foreign national visitors. Specifically, we contacted the Naval Sea Systems Command; the Space and Naval Warfare Systems Command; and the Space and Naval Warfare Command System Center, San Diego, California. The Navy had not published implementing policy on the DoD requirements for control of foreign national visitor access to LANs and for e-mail identification. As a result, the following situations existed.

- Of the 18 foreign national visitors assigned to NAVAIR headquarters at the time of our visit, 17 had unrestricted LAN accounts. The e-mail addresses for the 17 accounts did not identify them as belonging to foreign nationals

  A search of two NAVAIR LAN servers during our visit revealed examples of controlled unclassified information that had not been approved for release to foreign governments. Those examples included a test and evaluation master plan marked "Distribution to U.S. Government Agencies Only"; a Government cost estimate for a major weapon system marked "For Official Use Only - Not to be distributed without Program Office approval"; an aircraft component development specification marked "For Official Use Only"; and a specification marked "Contractor Proprietary."

- NAWCAD Instruction 5230.1A, "Visits and Assignments of Foreign Representatives," February 25, 1999, included DoD Directive 5230.20 requirements. However, as of November 1999, all 10 foreign national visitors assigned to NAWCAD research facilities, program offices, or the test pilot school had unrestricted accounts on the NAVAIR LAN and their e-mail addresses did not identify them as foreign nationals.

- A memorandum issued by the Commander, NAWCWD, "Access by Foreign Nationals Seeking Connectivity with NAWCWD Networks and Computing Devices," July 2, 1997, established policies for newly assigned foreign nationals at NAWCWD. The memorandum, which was superceded by NAWCWD Instruction 5239.4, "Network Security," December 1998, stated that network access by foreign nationals was to be granted on a case-by-case basis, subject to several restrictions. Foreign nationals requiring e-mail capability were to obtain that service through a commercial Internet provider.

  NAWCWD Instruction 5239.4 states: "No foreign national will be allowed unrestricted access to the NAWCWD network. Foreign nationals will only be permitted access to limited network services via network control devices approved by the NAWCWD, NSO [Network Security Office]." The NAWCWD information systems security manager stated that as of December 21, 1999, no foreign nationals had access to the NAWCWD LAN or military networks. Foreign nationals were provided stand-alone computers that could access commercial Internet service providers but could not access the NAWCWD LAN.

- As of December 20, 1999, approximately 50 foreign nationals assigned to Naval Sea Systems Command headquarters had unrestricted network accounts. Such unrestricted accounts could allow foreign nationals to access controlled unclassified and "No Foreign" information on three Navy Nuclear Propulsion Program networks. In September 1999, the Naval Sea Systems Command completed action to add a "FORN" suffix, plus the acronym identifying the Navy office to which a foreign national was assigned, to each foreign national's e-mail address.

  The e-mail address identification of foreign nationals is described in Management Policy and Standards, "Naval Sea Systems Command Global Exchange," version 2.0, October 20, 1999. That publication also describes an organizational e-mail distribution list hierarchy that places foreign nationals in a separate distribution list from Government employees and contractor personnel. As of December 20, 1999, the Deputy Chief Information Officer for Enterprise Operations, Naval Sea Systems Command, stated that a separate distribution list had not been established for foreign national visitors at the Naval Sea Systems Command.

- Foreign national visitors were assigned accounts on the Space and Naval Warfare Systems Command LAN when requested by their respective contact officers. As of February 4, 2000, 23 foreign national cooperative program personnel assigned to Space and Naval Warfare Systems Command headquarters had LAN accounts. An additional three foreign nationals assigned to the Systems Center in San Diego had LAN accounts.

Air Force Implementation of DoD Requirements

The Air Force had adequate procedures for assigning LAN access to foreign nationals. The Air Force had implemented the DoD requirements for controlling access to LANs at their laboratories and research facilities by foreign national visitors. Air Force direction is included in Air Force Instruction 33-202, "Communications and Information: Computer Security," February 1, 1999.

Air Force Policy. Air Force Instruction 33-202, section 3.7, "Foreign National Access to Air Force Information Systems," states:

> Authorizing access to SAF [Secretary of Air Force]-operated systems is delegated to the SAF assistant secretary level. Delegating authority for these positions shall not occur below the three-star level. MAJCOM [Major Command] commanders (MAJCOM/CC) are responsible for authorizing foreign national access to information systems within their respective commands. Delegating authority shall not occur below the MAJCOM vice commander.
>
> 3.7.1. Before authorizing foreign national access to specific information contained within an information system, the designees will:
>
> 3.7.1.1. Ensure the information is properly processed for disclosure.
>
> 3.7.1.2. Ensure systems accreditation authorities concur with the access.
>
> 3.7.1.3. Ensure the C&A [certification and accreditation] documentation for the system is updated to reflect foreign national access.
>
> 3.7.1.4. Ensure security measures employed adhere to information protection policy.

Air Force Materiel Command Policy. Air Force Materiel Command Policy Memorandum, "Foreign National Access to Unclassified Air Force Information Systems," September 30, 1999, directs implementation of Air Force Instruction 33-202. It delegates responsibility for authorizing foreign national access to the Vice Commander, Air Force Materiel Command. It also states that foreign national access to the Defense Information System Network must be validated by the Vice Commander and the Joint Staff, and approved by the Office of the Secretary of Defense. Specifically, the policy states, "The Servicing Foreign Disclosure Office will determine if the types/categories of information requested is releasable, prepare a memorandum explaining any specific requirements, and coordinate on the SSS [staff summary sheet] concurring or nonconcurring with the request."

Air Force Research Laboratory Policy. Air Force Research Laboratory Policy Directive 31-7, "Laboratory Security," August 1, 1999, states that DoD policies mandate a high degree of security throughout the acquisition process. The directive indicates that "heightened security awareness and threat-based countermeasures are essential during the R&D [research and development] phase when technology is most vulnerable to espionage, sabotage, and exploitation." It further states: "Each Laboratory Security Office will be the focal point for local technology protection efforts. Technology directors shall use the laboratory security as an extension of their staff to ensure all security disciplines are fully integrated into the Air Force Research Laboratory research and development program efforts."

The Air Force Research Laboratory's Director of Directed Energy issued a memorandum, "Procedures on Long-term Non-US Citizen Access to Government Facilities and Information," July 27, 1998. The memorandum states:

> Non-US citizen researchers will not be provided an account on AFRL [Air Force Research Laboratory] networks. An account or IP [Internet protocol] address on AFRL networks identifies the user as a '.mil' user. This is an erroneous identifier for non-US citizens. A '.mil' identifier allows the user access to restricted government sites beyond the scope of disclosure policies. For non-US visiting researchers who require access to the Internet, a justification as essential to duty performance must be submitted in writing to the FDO [Foreign Disclosure Office] through the OPSEC [Operational Security] Manager and Division Security Specialist. Once approved by the Division Chief, access to the Internet will be via a commercial account on a stand-alone computer only. Any other type of access will require a risk assessment and coordination between the Chief Information Officer, Security and OPSEC Managers.

Air Force Actions. The Air Force Research Laboratory sites visited had implemented the requirement in DoD directives on delegation of approval authority for assigning LAN accounts to foreign national visitors. In addition, the DoD requirements for identification of foreign nationals in electronic communications were addressed.

Summary

DoD directives require controls on access by foreign national visitors to AISs unless the systems have been sanitized or configured to ensure that a foreign national's access to classified and controlled unclassified information is limited to that which has been authorized for release to his or her government. LANs, which are accessed using AISs, may contain controlled unclassified information. Examples of such controlled unclassified information were found on Navy LANs. The Army and the Navy had not implemented required access controls. However, the Air Force had implemented controls. In addition, the Navy had not implemented a DoD directive requiring identification of foreign nationals in

e-mail communications. As a result, the Army and the Navy had no assurance that controls over foreign national visitors were adequate to protect against unauthorized access, through LANs or e-mail communications, to militarily sensitive technologies and information.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Army Deputy Chief of Staff for Intelligence revise Army Regulation 380-10, "Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives," and the Army Director of Information Systems for Command, Control, Communications, and Computers revise Army Regulation 380-19, "Information Systems Security," to incorporate the requirements of the Army memorandum, "Foreign Representative Access to Army Computers and Computer Networks Interim Policy," to:

a. Provide verifiable assurance that foreign national visitors are unable to access unauthorized technologies and technical information through local area networks.

b. Delineate clear policy and an Army-wide standard format to implement the requirement in DoD Directive 5230.20 for identification of foreign nationals in e-mail communications.

Management Comments. The Office of the Director of Information Systems for Command, Control, Communications, and Computers, concurred with the finding and the recommendation to update Army Regulation 380-19, stating the recommended changes are incorporated in Army Regulation 25-XX, scheduled to replace Army Regulation 380-19 in October 2000. The new regulation will also establish an Army-wide format to meet the requirements in DoD Directive 5230.20 for identification of e-mail communications.

Audit Response. The Army response to the recommendation is not fully responsive. Office of the Director of Information Systems for Command, Control, Communications, and Computers comments concerning Army Regulation 380-19 were responsive. However, that office does not have purview over Army Regulation 380-10 and, therefore, could not respond concerning changes to that regulation. We ask that the Army Deputy Chief of Staff for Intelligence provide comments on the final report.

2. We recommend that the Navy Chief Information Officer and the Office of the Chief of Naval Operations revise Secretary of the Navy Instruction 5239.3, "Department of the Navy Information Systems Security Program"; Secretary of the Navy Instruction 5510.36, "Department of the Navy Information Security Program Regulation"; and Chief of Naval Operations Instruction 5239.1B, "Navy Information Assurance Program," to:

a. Delineate clear policy and implementation of the requirement in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," for DoD Component heads to approve assignment of local area network accounts to foreign nationals.

b. Direct the immediate revocation of access by foreign nationals to local area networks for which controls have not been implemented to prevent unauthorized access to controlled unclassified information that may be available on those networks.

c. Delineate clear policy and procedures for implementing the requirement in DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals," for sanitization or configuration changes of automated information systems to prevent unauthorized access to classified and controlled unclassified information by foreign nationals.

d. Delineate clear policy and a Navy-wide standard format to implement the DoD requirement in Directive 5230.20 for identification of foreign nationals in e-mail communications.

3. We recommend that the Director, Navy International Programs Office, in coordination with the Navy Chief Information Officer, revise Secretary of the Navy Instruction 5510.34, "Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations," to reference and reemphasize the policies and procedures, including e-mail identification of foreign nationals, in the revised Secretary of the Navy Instructions 5239.3 and 5510.36 and the revised Chief of Naval Operations Instruction 5239.1B.

Management Comments. The Navy did not comment on Recommendation 2. or Recommendation 3. in a draft of this report. We request that the Navy provide comments on the final report.

Appendix A. Audit Process

Scope

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with the National Defense Authorization Act for Fiscal Year 2000, section 1402, which requires an annual report on the transfers of militarily sensitive technology to countries and entities of concern.

We reviewed and evaluated the adequacy of DoD and Military Department directives, policies, regulations, memorandums and letters of instruction implemented during the period 1981 through 1999, related to preventing the inappropriate transfer of sensitive and critical technologies with potential military application to countries and entities of concern.

We conducted interviews with personnel at the Office of the Under Secretary of Defense for Policy; the Deputy Under Secretary of Defense (Science and Technology); the Director, Defense Research and Engineering; the Military Departments; the Director, Defense Threat Reduction Agency; and the DoD program offices. In addition, we visited research facilities at the Army Armament Research, Development and Engineering Center; the Army Communications-Electronics Command; NAVAIR; NAWCAD; NAWCWD; and the Air Force Research Laboratories at Wright-Patterson and Kirtland. At those sites, we conducted interviews with DoD managers responsible for managing the technology security programs and for managing and controlling foreign national visitors. We also interviewed officials at the Naval Sea Systems Command; the Space and Naval Warfare Systems Command; and a Space and Naval Warfare Systems Center.

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal, subordinate goal, and performance measure:

> **FY 2000 Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve the 21st century infrastructure. **(00-DoD-2)** **FY 2000 Subordinate Performance Goal 2.2:** Transform the U.S. military forces for the future. **(00-DoD-2.2)** **FY 2000 Performance Measure 2.2.2:** Status of Defense Technology Objectives as Judged by Technology Area Review Assessments. **(00-DoD-2.2.2)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal:

> **Information Technology Management Functional Area.**
> **Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

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

Methodology

Audit Approach. For each site visited, we:

- reviewed approval procedures for authorizing foreign visitors and for clearing the foreign visitor at the location;
- identified foreign visitors from countries and entities of concern;
- identified the programs, technologies, and information that were accessible to the foreign visitors;
- reviewed information systems security and physical security controls applicable to the foreign visitor;
- interviewed security officials and foreign national visitor control officials responsible for monitoring and escorting foreign national visitors during visits;
- reviewed case files for foreign national visitors to the laboratories and program offices visited; and
- performed tests to ensure proper implementation of those policies and procedures.

Audit Type, Dates, and Standard. We performed this program audit from August 1999 through February 2000 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Accordingly, we included tests of management controls considered necessary. We did not use computer-processed data to perform this audit.

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

Management Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of those controls.

Scope of Review of the Management Control Program. We reviewed the adequacy of management controls over information systems security as well as personnel and physical security at the Army Materiel Command and NAVAIR organizations visited. Specifically, we reviewed the management controls over LAN accounts, identification badges, vehicle decals, escort requirements, and checkout procedures for foreign nationals on extended visits. We also reviewed implementation of Air Force Instruction 33-202 and Army and Navy Annual Statements of Assurance for FY 1998 and FY 1999. Because we did not identify a material weakness, we did not assess management's self-evaluation.

Adequacy of Management Controls. The procedural deficiencies indicated by the audit are management control weaknesses, but we did not regard them as material, as materiality is defined in DoD Instruction 5010.40. Nevertheless, they need to be addressed. The recommendations made in this report will, if implemented, eliminate the procedural deficiencies.

Appendix B. Prior Coverage

During the last 5 years the General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to the adequacy of management controls over transfers of sensitive and critical DoD technology with potential military application to foreign nationals. Unrestricted General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Unrestricted Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil. The following previous reports are of particular relevance to the subject matter in this report.

General Accounting Office

General Accounting Office Report No. NSIAD-98-196 (OSD Case No. 1648), "Export Controls: Information on the Decision to Revise High Performance Computer Controls," September 1998.

General Accounting Office Report No. NSIAD-95-82 (OSD Case No. 9798), "Export Controls: Some Controls Over Missile-Related Technology Exports To China Are Weak," April 1995.

Inspector General, DoD

Inspector General, DoD, Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000.

Inspector General, DoD, Report No. 98-214, "Implementation of the DoD Technology Transfer Program," September 28, 1998.

Inspector General, DoD, Report No. 98-157, "Updating the Foreign Disclosure and Technical Information System," June 17, 1998.

Inspector General, DoD, Report No. 97-210, "Technology Transfer Under the F-15I Program," August 27, 1997.

Interagency Reviews

Inspectors General of the Departments of Commerce, Defense, Energy, and State, Report No. D-2000-109, "Interagency Review of the Export Licensing Process for Foreign National Visitors," March 2000.

Interagency Reviews (cont'd)

Inspectors General of the Departments of Commerce, Defense, Energy, State, and the Treasury and the Central Intelligence Agency, Report No. 99-187, "Interagency Review of the Export Licensing Processes for Dual-Use Commodities and Munitions," June 18, 1999.

Appendix C. Other Matters of Interest

The Deputy Secretary of Defense took several completed and ongoing actions to address counterintelligence and security concerns at DoD research facilities. This appendix discusses some of those actions and our review of physical security at the research facilities we visited or contacted.

Deputy Secretary of Defense Taskings. On January 28, 1999, the Deputy Secretary of Defense requested that managers of technology organizations certify certain practices in counterintelligence and security at the DoD research facilities they manage. Results did not identify any serious systemic issues. On March 19, 1999, the Deputy Secretary of Defense requested that each Military Department Inspector General conduct an assessment of counterintelligence and security practices at selected research facilities and test centers. The Inspectors General reported their findings and made recommendations for follow-on actions. Most recommendations to improve security were either implemented on the spot or were planned for implementation by the organizations involved. Other recommendations affecting research facilities required further coordination effort. As a result, in August 1999, the Deputy Secretary of Defense directed the establishment of an Overarching Integrated Process Team to develop actions to improve counterintelligence and security practices at research facilities. The Overarching Integrated Process Team is composed of representatives of the Services and other DoD organizations performing research, development, test, and evaluation.

Five general areas were identified for improvement:

- training;
- counterintelligence link to research, development, test, and evaluation;
- visitor handling;
- security and counterintelligence integration; and
- budget incentives.

In response to the Overarching Integrated Process Team, the Deputy Under Secretary of Defense (Science and Technology) prepared five memorandums. On February 17, 2000, the memorandums were signed by the Deputy Under Secretary of Defense (Science and Technology). The memorandum for the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) directs actions on initiatives to improve counterintelligence, to improve the generation and flow of information to protect research and technology, and to increase security awareness and skills in technology protection. Included in the initiatives were a "standardized automated entry badge system for the Department that will electronically log and centrally track RDT&E [research, development, test, and evaluation] site visitor access,

including foreign visitors," as well as improvements for "visually distinguishing badges provided to foreign visitors and decals provided for their registered vehicles."

Implementation of the Deputy Secretary of Defense initiatives will address the similar areas of concern we identified at the six research facilities we visited or contacted. Areas of concern included badging, vehicle decal identification, escort requirements, and checkout procedures.

Badging

Standard DoD badging procedures for foreign national visitors did not exist. The procedures varied at all six sites visited. Differences also existed between research facilities located at the same site. Each site differed on the types of badges issued; the length of time a badge could be issued for; whether long-term visitors were allowed to keep their badges when they returned to their home country for a visit; and when and if the badges were collected. Following are specific examples.

- The Army Armament Research, Development and Engineering Center did not use a badge or pass system for 1 day and recurring short-term foreign national visits, but relied on enforced escort procedures.

- The Army Communications-Electronics Command did not use a standard badge throughout the command, but each building separately issued badges to foreign national visitors.

- NAWCAD and NAWCWD used a wide range of badges, from paper or laminated badges with no pictures to plastic multicolor-coded badges with pictures and country flags. Some badges had control numbers; others did not. The length of time for which a badge could be issued also varied. Further, there were instances where long-term visitors were allowed to keep their badges when they returned to their home country for a visit.

- The Air Force research laboratories issued distinctive badges to some foreign nationals, while others were issued electronic swipe badges that limited access to unauthorized locations and automatically deactivated on the last day of the approved visit.

Vehicle Decal Identification

We could not identify any guidance that specifically addressed the registration and marking of vehicles owned and operated by long-term foreign national visitors. At the sites visited, the following practices were observed.

- The Army had no requirement to register and distinguish a foreign visitor's vehicle from others on the installation.
- The Navy issued vehicle decals to long-term foreign nationals that did not differentiate the foreign national visitor from civilian or military employees.
- The Air Force had no written procedures concerning the issuance of vehicle decals to foreign national visitors. However, civilian and military employees were issued vehicle decals, while foreign nationals were not issued vehicle decals.

Escort Requirements

There were no standard criteria, in regards to countries of concern, for when a foreign national visitor should be escorted. Not only did the Military Departments follow different procedures, but research facilities within a department also varied, as illustrated in the following examples.

- At the Army Armament Research, Development and Engineering Center, escort requirements were not being enforced for long-term foreign national visitors. One long-term foreign national visitor was allowed to host tours, including restricted areas, for other foreign national visitors. An escort was not required, although access to the restricted areas required someone to allow them in.
- At NAWCAD, which integrated foreign national into the work force, long-term foreign national visitors were issued "no-escort required" badges for their respective program offices. However, by not requiring an escort, access to other program offices could not be regulated because most of the program offices were located in the headquarters building of NAVAIR.
- At NAWCWD, foreign nationals were not integrated into the work force but were segregated to assigned workspace in trailers. Each foreign national was provided a security plan, which described in detail where the foreign national could travel without an escort, usually from the installation front gate to the assigned workspace.
- At the Air Force research laboratories, foreign national visitors were not integrated into the work force and a security plan was used.

Checkout Procedures

Each site visited had checkout procedures for civilian and military personnel. Those procedures normally consisted of checklists requiring certain actions to be taken, including the return of Government property, such as credit cards or keys. We could not identify any standard checkout procedures for foreign national visitors that ensured the collection of long-term badges, vehicle decals, keys, and phone cards or the termination of e-mail accounts.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
  Director, Defense Research and Engineering
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense for Policy
  Assistant Secretary of Defense (International Security Affairs)
  Deputy Under Secretary of Defense (Policy Support)
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Security and Information Operations)

Department of the Army

Deputy Under Secretary of the Army (International Affairs)
Commanding General, Army Materiel Command
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Director, Navy International Programs 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)
Deputy Under Secretary of the Air Force (International Affairs)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, Defense Security Cooperation Agency

Other Defense Organizations (cont'd)

Director, Defense Systems Management College
Director, Defense Threat Reduction Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center

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 Banking
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
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
House Committee on International Relations
House Subcommittee on International Economic Policy and Trade, Committee on International Relations
House Permanent Select Committee on Intelligence

Department of the Army Comments

Office, Director of Information Systems for Command, Control, Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

17 MAY 2000

SAIS-IAS (36-2c)

MEMORANDUM FOR Inspector General, Department of Defense, ATTN: LAIG-AUD-RLS, 400 Army Navy Drive, Arlington, VA 22202-2885

SUBJECT: DoD-IG Draft Audit Report: Foreign National Access to Automated Information Systems, Project No. 9LG-5030.01

The Army reviewed the subject draft report, and agrees with the DoD-IG finding and recommendation.

Finding: The Army did not have adequate procedures for assigning LAN accounts to foreign nationals because the DoD requirement to control foreign visitor access to information on LANs had not been implemented by the Army. However, the Army had implemented the DoD requirement for control of foreign nationals through foreign identification in e-mail address.

COMMENT: Concur with recommendation 1. Army Regulation 380-19 is being revised, and will be renumbered as Army Regulation 25-xx(to be determined). Target publication date is October 2000. It incorporates Army interim policy, provides verifiable assurance that foreign national visitors are unable to access unauthorized technologies and technical information through local area networks, and establishes an Army-wide format to meet the requirements in DoD Directive 5230.20 for identification in e-mail communications.

Additional information may be obtained from Ms. Angelique Woodson at (703) 695-4074, e-mail angelique.woodson@hqda.army.mil, or LTC Robert J. Bollig at (703) 607-5887, e-mail robert.bollig@hqda.army.mil.

RICHARD W. SOHM
Deputy Director, Information Assurance

Printed on Recycled Paper

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Shelton R. Young
Evelyn R. Klemstine
Mary E. Geiger
Jane T. Thomas
Julie C. Kienitz
David L. Leising
Woodrow W. Mack

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Foreign National Access to Automated Information Systems

B. DATE Report Downloaded From the Internet: 06/05/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 06/05/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.