



**DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010**

FEB 17 2000

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (POLICY)

SUBJECT: Policies for Technology Protection

This past May inspections of security and counterintelligence practices at Department of Defense (DoD) sites conducting research, development, test and evaluation (RDT&E) identified several practices that could be adjusted to improve the Department's ability to protect technologies under development or test at our research and development laboratories and test and evaluation centers. In August I chartered an overarching integrated process team (OIPT), chaired by the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)) and including a representative from your office, to develop proposals for improvement in several areas identified by inspectors. You are assigned primary or lead responsibility for actions listed below, and you should assist others in carrying out their supporting functions.

I direct action on the following initiatives to adjust current policies regarding technology protection and training:

- a. amend DoD Directive 5230.20 to require that certain foreign visits to DoD Component facilities, now exempted from procedures for the International Visits Program, are recorded in the DoD Foreign Visits System (FVS);
- b. with support of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence (ASD (C3I)) and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)), establish FVS terminals at RDT&E sites for visitor data entry where applicable; and,
- c. working with ASD (C3I), identify and implement additional FVS data fields useful for counterintelligence purposes.

Your actions will contribute to creation of new information flows among a team of well-trained professionals for RDT&E technology protection. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. If you have any questions on the initiatives outlined above, please call Dr. John Tangney, Office of the Deputy Under Secretary of Defense (Science and Technology), 697-9215.


John J. Hamre



I-00/002215
119300 / 99



POLICY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

June 22, 2001

MEMORANDUM FOR DIRECTOR FOR COUNTERINTELLIGENCE, OASD/C3I

SUBJECT: Confirmation of Foreign Visitors Requirement

Dave

We have been working for the past year gathering requirements for what we call the Confirmation Foreign Visits System (CFVS) to meet guidance in earlier DEPSECDEF memoranda. During this period we have made great inroads in defining the process and understanding responsibilities. During recent action officer level coordination meetings with your office, it was agreed that the CFVS would be designed to confirm a foreign visitors arrival relating to an FVS approved visit and be capable of creating new visitor records for those visitors outside the scope of the FVS. It was also agreed that CI subjective information to be collected on foreign visitors would be collected by CI assets and entered directly onto a CI system that will be developed. A list of these data elements is enclosed.

During our analysis of the original confirmation requirement, we decided to expand the capabilities of CFVS to support additional local site requirements for typical "check-in" control information on foreign visitors, thereby automating local visitor log capabilities. Use of this local logging would be an optional feature. In doing so we identified additional fields users require to meet local physical security policies. These are also listed in the enclosure.

We ask that you review these additional fields to determine if you would like this information to be transferred to your CI network along with other information in FVS and CFVS that you previously identified. We also ask that you review the above responsibilities on subjective CI data collection and comment or concur as appropriate about the automated collection responsibilities since this represents a slight change from the DEPSECDEF assignment of automation responsibilities.

*Thax
Ron*

Ronnie R. Larson
Director, Policy Automation
Office of the Deputy Under Secretary of Defense
(Policy Support)

Attachment
As Stated

CC: International Security Policy Directorate



Data Elements for Foreign Visitor CI and Visitor Control Databases

1. The responsibility for automation of data identified as required for CI analysis is as follows:

Policy AutomationC3I

Actual Visit Start Date/*time*
 Actual Visit End Date/*time*
 Unannounced Visit Indicator Code
 Visitor VISA Number (Optional)
 Visitor Maiden Name (Optional)
 FVS Case ID
 Visitor Rank/Name
 Visitor Date of Birth
 Visitor Place of Birth
 Visitor ID/PPN
 Visitor Nationality
 Visitor Security Clearance
 Visit Start Date
 Visit End Date
 Visit Type -
 Facility Name
 US Facility POC Name
 US Facility POC Phone Number

Unusual Visitor Behavior Report
 Unusual Visitor Behavior Report Date
 Other Place(s) Visited by Visitor
 Date(s) of Other Place(s) Visited
 Status of Visitor at Other Places Visited
 Visitor Technical Expertise Code
 Visit Technology Category Code

Visitor ~~Home~~ Sponsoring Country
 Visit Purpose

2. The following are additional fields of information CFVS will be collecting for local visitor control that C3I may be able to use for CI analysis and therefore could be passed along with the other information :

Visitor Hair Color
 Visitor Eye Color
 Visitor Weight
 Visitor Height.
 Visitor Badge #
 Visitor Sex



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 17 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, BALLISTIC MISSILE DEFENSE ORGANIZATION
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, ARMED FORCES RADIOBIOLOGY RESEARCH
INSTITUTE

SUBJECT: Security and Counterintelligence in Laboratories and Centers

This past January I asked managers of technology organizations to certify certain practices in security and counterintelligence at sites they manage. Results indicated that more could be done to achieve greater consistency of security and counterintelligence practices. In response, inspections of Research, Development, Test and Evaluation (RDT&E) sites were conducted to further validate baseline security and counterintelligence practices. These inspections, conducted largely by the Inspectors General of the Military Departments, produced many findings that were followed up by each of the Military Departments. Other findings, however, required a more broadly coordinated approach.

In July, I appointed an overarching integrated process team (OIPT), chaired by Deputy Under Secretary of Defense for Science and Technology (DUSD)(S&T) with senior representatives of the Military Departments and the Office of the Secretary of Defense (OSD), to propose actions that address specific security and counterintelligence practices in the RDT&E organizations. Recommendations of the OIPT for security and counterintelligence at laboratories and centers are reflected in the attached memoranda.

The attached memoranda direct a number of actions that will require coordinated effort of several organizations to achieve desired capabilities in technology protection. Your action is requested to ensure that the stakeholder communities of security, counterintelligence, and acquisition work with the OSD offices addressed in the attached memoranda. The initiatives described are scheduled for implementation within the year. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. Additional information on these initiatives is available from Dr. John Tangney, ODUSD (S&T), 703-697-9215.


John J. Hamre

Attachments:
As stated



U19300 / 99



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 17 2000

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

SUBJECT: Security and Counterintelligence Practices at Laboratories and Centers

This past May inspections of security and counterintelligence practices at Department of Defense (DoD) sites conducting research, development, test and evaluation (RDT&E) identified several practices that could be modified to improve the Department's ability to protect technologies under development or test at our research and development laboratories and test and evaluation centers. In August I chartered an overarching integrated process team (OIPT), chaired by the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)) and including a representative from your office, to develop proposals for improvement. You are assigned primary or lead responsibility for actions listed below, except as otherwise indicated, and you should assist others in carrying out their supporting functions.

I direct continued action on the following counterintelligence initiatives:

- a. increase the collection of counterintelligence (CI) threat data;
- b. enhance tools for CI threat analysis;
- c. assign CI specialists in the Military Departments to provide full-time, dedicated CI support to research and technology protection at all major RDT&E sites and ensure all other sites receive appropriate levels of CI support; and
- d. shape a program of integrated CI support to RDT&E sites.

Action to implement this program of integrated support, expressed as "contracts" of support for individual RDT&E sites, is central to other initiatives and is listed first among those following.

I direct action on the following initiatives designed to improve generation and flow of information for research and technology protection at RDT&E sites:

- a. with support of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)), implement a new program of integrated support for RDT&E sites, including site-specific technology protection plans that identify critical program information for non-Science and Technology (S&T) programs, and a process for assessment of this new program;
- b. enhance flow of threat data to RDT&E sites;



- c. implement a standardized automated entry badge system for the Department that will electronically log and centrally track RDT&E site visitor access, including foreign visitors;
- d. with support of the Under Secretary of Defense for Policy (USD (P)), enable entering of foreign visit data at RDT&E sites for centralized analysis of these and other data;
- e. improve systems for visually distinguishing badges provided to foreign visitors and decals provided for their registered vehicles; and,
- f. with support of the USD (P) and the USD (AT&L), revise or create DoD Directive to define a new program of integrated support for technology protection at RDT&E sites, to include codifying workforce training requirements for security awareness.

I direct action on the following initiatives designed to increase security awareness and skills in technology protection:

- a. automate the delivery of existing RDT&E workforce training programs (including training on release to media and the early determination of program sensitivity);
- b. train CI personnel for work in RDT&E settings;
- c. train security personnel for integrated RDT&E support;
- d. in conjunction with the USD (AT&L), increase program manager training for technology protection; and,
- e. in conjunction with the USD (P), codify workforce training requirements for RDT&E technology protection.

These initiatives will help to protect the technology-dependent cutting edge of our weapons systems. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. If you have any questions on these initiatives, please call Dr. John Tangney, ODUSD (S&T), 697-9215.



John J. Hamre

cc:

Inspector General, DoD

Director, OT&E

Secretaries of Military Departments

USD (AT&L)

USD (P)



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 17 2000

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION,
TECHNOLOGY, AND LOGISTICS)

SUBJECT: Technology Protection

This past May inspections of security and counterintelligence practices at the Department of Defense (DoD) sites conducting research, development, test and evaluation (RDT&E) identified several practices that could be adjusted to improve the Department's ability to protect technologies under development or test at our research and development laboratories and test and evaluation centers. In August I chartered an overarching integrated process team (OIPT), chaired by the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)), to develop proposals for improvement in several areas identified by inspectors. You are assigned primary or lead responsibility for actions listed below, and you should assist others in carrying out their supporting functions.

I direct action on the following initiatives designed to improve technology protection of acquisition programs, including protection at RDT&E sites:

- a. in support of ASD (C3I), implement a new program of integrated support to tailor technology protection for individual RDT&E sites, including development of site-specific lists of critical program information for non-S&T programs;
- b. within normal reviews of acquisition programs, increase emphasis on program manager accountability for successful execution of program protection plans; and,
- c. with support of ASD (C3I), modify courses for program managers and other acquisition leaders at the Defense Acquisition University to include more information concerning the role of counterintelligence in technology protection.

These initiatives will help protect the technology-dependent cutting edge of our weapons systems. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. If you have any questions on these initiatives, please call Dr. John Tangney, Office of the Deputy Under Secretary of Defense for Science and Technology, 697-9215.


John J. Hamre



cc:

ASD (C3I)

Director, OT&E

Secretaries of Military Departments

USD (P)

Inspector General, DoD



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 17 2000

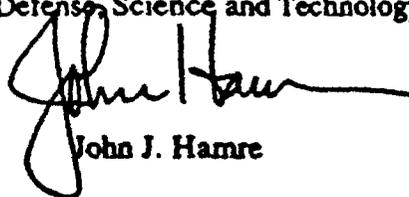
MEMORANDUM FOR ACTING INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Inspection of Security and Counterintelligence Practices at Laboratories and Centers

In response to findings from inspections of security and counterintelligence practices at research, development, test and evaluation (RDT&E) sites, an overarching integrated process team (OIPT) chaired by the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)) has developed several initiatives for improved practices. An initiative involving continued regular inspections of RDT&E sites has been accepted.

Accordingly, I request the Department of Defense (DoD) Inspector General to ensure a uniform system of periodic reviews through the existing agency and service inspection processes for compliance with directives concerning security, technology protection, and counterintelligence practices. Such reviews should be integrated with current inspection programs of the Military Services, and review results should be shared with command elements having policy or oversight roles in technology protection. It is also requested that you develop inspection list guidelines for department-wide Inspectors General to enhance consistency across the DoD. Inspection checklists may take advantage of site-specific technology protection plans to be produced as part of another initiative led by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)).

These reviews will help protect the technology dependent cutting edge of our weapons systems. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. If you have any questions on the inspection initiative outlined above, please call Dr. John Tangney, Office of the Deputy Under Secretary of Defense, Science and Technology, 697-9215.



John J. Hamre

cc:
ASD (C3I)
Director, OT&E
Secretaries of Military Departments
USD (AT&L)
USD (P)





DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 17 2000

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (POLICY)

SUBJECT: Policies for Technology Protection

This past May inspections of security and counterintelligence practices at Department of Defense (DoD) sites conducting research, development, test and evaluation (RDT&E) identified several practices that could be adjusted to improve the Department's ability to protect technologies under development or test at our research and development laboratories and test and evaluation centers. In August I chartered an overarching integrated process team (OIPT), chaired by the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)) and including a representative from your office, to develop proposals for improvement in several areas identified by inspectors. You are assigned primary or lead responsibility for actions listed below, and you should assist others in carrying out their supporting functions.

I direct action on the following initiatives to adjust current policies regarding technology protection and training:

- a. amend DoD Directive 5230.20 to require that certain foreign visits to DoD Component facilities, now exempted from procedures for the International Visits Program, are recorded in the DoD Foreign Visits System (FVS);
- b. with support of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence (ASD (C3I)) and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)), establish FVS terminals at RDT&E sites for visitor data entry where applicable; and,
- c. working with ASD (C3I), identify and implement additional FVS data fields useful for counterintelligence purposes.

Your actions will contribute to creation of new information flows among a team of well-trained professionals for RDT&E technology protection. The OIPT will meet twice a year to prepare updated reports on the progress of these initiatives. If you have any questions on the initiatives outlined above, please call Dr. John Tangney, Office of the Deputy Under Secretary of Defense (Science and Technology), 697-9215.


John J. Hamre



cc:

ASD (C3I)

Director, OT&E

Secretaries of Military Departments

USD (AT&L)

Inspector General, DoD



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 31 2000



MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION,
TECHNOLOGY AND LOGISTICS)
UNDER SECRETARY OF DEFENSE (POLICY)
ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS AND INTELLIGENCE)

SUBJECT: Technical Measures to Support Identification and Positive Control of
Foreign Visitors

This past February I issued guidance to adjust current policies regarding technology protection. These adjustments addressed, in part, foreign visits to Department of Defense (DoD) Component facilities. I want to extend my guidance to further expand the use of information technology and biometrics to facilitate the identification and positive control of foreign visitors. Accordingly, I direct action on the following initiatives designed to improve visitor control at sensitive DoD facilities including research, development, test and evaluation (RDT&E) sites:

- a) The Under Secretary of Defense for Policy (USD(P)), with support from the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), will examine policies that will provide for the identification and control of pertinent foreign visitors to sensitive DoD sites including through the use of biometrics technology and will determine the international policy concerns and considerations related to its use.
- b) The USD(AT&L) will develop and implement a pilot program demonstrating the use of biometrics technology for foreign visitor identification and positive control at a DoD laboratory installation and report on the technical viability of the approach and any unresolved issues at the completion of the pilot program.
- c) The USD(P), together with the ASD(C3I), will develop detailed architecture for integration of expanding the Foreign Visits System (FVS) to record all designated foreign visitors. Consideration should be given to interfacing the system with those of other Departments and Agencies as appropriate.
- d) Together, the USD(AT&L), the USD(P), and the ASD(C3I) will recommend within 180 days a detailed architecture and acquisition strategy, to include costing, for an augmented FVS consistent with the outcomes of the above efforts.

The above initiatives will greatly assist the protection of military related technology and will ultimately contribute to the maintenance of our cutting edge in weapons systems.


John J. Hamre

U04716 /00

Toby



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



MAY 12 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Foreign Visits System and Reporting of Foreign National Visitors to DoD Installations and Facilities and to DoD Cleared Contractor Facilities

The DoD International Visits Program, the Foreign Liaison Officer Program and the Defense Personnel Exchange Program were established to process requests for visits by and assignments of foreign nationals to the DoD Components and DoD contractor facilities. They are designed to ensure that classified and controlled unclassified information to be disclosed to them has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a security assurance on the individuals when classified information is involved in the visit or assignment, and to facilitate administrative arrangements, such as ensuring that the visit or assignment can be accommodated from a legal and support perspective.

In order to manage better visits and assignments of foreign nationals under these programs and to ensure that access to classified and unclassified export controlled information has been properly authorized, DoD needs to maintain records concerning persons who actually visit or are assigned pursuant to an approved authorization. Records also must be maintained of visits that have not been processed through the Foreign Visits System (FVS). Accordingly, effective immediately, DoD Components shall record all visits or assignments of foreign nationals to their facilities. In addition, the Under Secretary of Defense for Policy (USD(P)) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) shall develop a proposal for automated reporting of this information to the FVS. ASD(C3I) shall include estimates of manpower and financial resources that would be required in a recommendation to me concerning the possible implementation of such an automated reporting system, along with a recommendation for acquiring the necessary resources.

In addition, to ensure effective implementation of DoD policies for control of foreign nationals visiting or assigned to DoD Components and DoD contractor facilities, addressees shall review their policies for the control of foreign nationals visiting or assigned to their facilities. Addressees shall provide to the USD(P), within sixty days of the date of this memorandum, a report on procedures that have been developed and implemented to comply with DoD Directive 5230.20, "Visits, Assignments and Exchanges of Foreign Nationals," August 12, 1998. A copy of Component implementing

U06116 /00

procedures will suffice. Addressees also shall provide to the Deputy to the Under Secretary of Defense (Policy) for Policy Support, within forty-five days of the date of this memorandum, comments on those aspects of DoD Directive 5230.20 that are not clear or that may need streamlining.

In order to ensure that established U.S. laws and national and DoD regulations and policies concerning the protection and disclosure of classified and unclassified export controlled information are applied uniformly to all foreign nationals visiting or assigned to DoD Component and DoD contractor facilities, Section 2.3 of DoD Directive 5230.20 shall be amended to read: "Visits in the following categories will not be processed using the Foreign Visits System (see subsection 5.2.3, below). Nevertheless, DoD Components shall apply controls to ensure that all visitors who fall within the categories below do not gain unauthorized access to classified or unclassified export controlled information or work areas where such information resides."

DoD Directive 5230.20 shall be amended accordingly.



Rudy de Leon



THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

24 October 2001

In Reply, Refer To:
01/012767

MEMORANDUM FOR DOD INSPECTOR GENERAL
ATTN: MR. E. J. FISHER

SUBJECT: Follow-up on OIG Report No. 98-157

This memorandum responds to questions from the DoD IG memorandum of 16 Oct 01, same subject, as follows:

IG Question: Was the off-line Foreign Disclosure capability (FDS) creation capability deployed on schedule in June 2001?

Response: The Policy Automation Directorate (PAD) did not meet the June 2001 schedule. We did deploy the off-line FDS to six selected DoD sites during the week of 8 October 2001. Our plan is to complete the deployment to all activities by the end of December 2001.

IG Question: Discuss the status of your initiative to redesign the Embassy portion of FDS and provide the current schedule for releasing this capability.

Response: We have not started this project as yet due to more pressing priorities and have not established an implementation schedule. Due to recent events our priority is now on controlling foreign visitors and streamlining export license requests. However, we believe we can begin the redesign of the Embassy portion of FVS in December 2001 with an estimated completion date of 31 March 2002.

If you have any questions please contact Mr. Jack Farmerie, 697-5496.

Ronnie R. Larsen
Director, Policy Automation
Office of the Deputy Under Secretary of Defense
(Policy Integration)





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

APR 9 2002

MEMORANDUM FOR AUDIT FOLLOWUP FOCAL POINT, ASSISTANT FOR
ADMINISTRATION, (USD(P))

SUBJECT: Followup on **OIG Report No. 98-157**, "Updating the Foreign Disclosure
and Technical Information System," June 17, 1998

Pursuant to the requirements of DoD Directive 7650.3, the subject case is being evaluated to ensure that adequate management action is taken on the report's agreed-upon finding and recommendations. Followup status will be reflected in our Defense Audit Management Information System (DAMIS) and, as appropriate, in reports to the Secretary of Defense, GAO and the Congress.

Based on your October 24, 2001 status update (enclosed), additional information is required to document the status of corrective action on Recommendation 1 (page 10) in the subject report. Accordingly, request you specifically address the following:

Has the Foreign Disclosure System of-line capability been fully deployed? If not please explain and project when this action will be complete.

Discuss the status of action to redesign the Embassy portion of Foreign Visits System (FVS). You estimated that redesign of the Embassy portion of FVS would begin in the December 2001 timeframe and that this action would be complete by March 31, 2002. Discuss your current plans for releasing this redesigned capability. If this action has been further delayed, please explain and provide an extended completion date.

Please forward the requested information to us by **May 13, 2002**. Mail should be addressed to the DoD Inspector General Attn: AFTS, 400 Army Navy Drive, and may be forwarded through the OSD Mail Room, 3A948, the Pentagon. The action officer for this case is Mr. E. J. Fisher, 703-604-9645.

A handwritten signature in black ink, appearing to read "Carlos J. Chapa".

Carlos J. Chapa
Technical Director
Audit Followup & GAO Affairs

Enclosure

I-02/005663