

Office of INSPECTOR GENERAL

Audit Report

*Review of USITC's Information
Security Program*

Report No. IG-07-90



September 1990

Date Issued



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

September 28, 1990

REVIEW OF USITC'S INFORMATION SECURITY PROGRAM

The objective of this review was to evaluate the Commission's compliance with Executive Order 12356, National Security Information, and the implementing directives issued by the National Security Council and Information Security Oversight Office (ISOO) of the General Services Administration. The Executive Order provides that each agency should establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

We found that the Commission has developed an information security program with policies and procedures generally consistent with the Executive Order and implementing ISOO regulations. In some instances, compliance with the policies and procedures is substantial, as in using proper security containers and signing Nondisclosure Agreements.

However, we identified multiple areas that are not material where policies and procedures need to be refined and compliance increased in order to fully comply with the provisions of the Executive Order and ISOO regulations. Our findings in these areas are:

- The Commission issues the same type of identification badges to individuals with and without security clearances (page 4);
- Physical security included weaknesses such as: the primary control to ensure combinations were changed as required did not clearly include all security containers, combinations were being changed by locksmiths without security clearances, offices generally did not use an accountability log, the annual inventory did not include responses from all offices or all required categories of classified documents, inadequate controls over burn bags, particularly that they were given to a contractor without a security clearance, and that records were not maintained on destruction of Secret documents (pages 5-8);
- Some of the standard forms for document security were used sporadically (pages 9-11);

- Confidential reports and workpapers were not marked in accordance with current guidance (pages 11-12);
- The Security Education Program does not include termination or foreign travel briefings, and the refresher briefing was last offered over a year ago and not attended by all employees (pages 12-15);
- The Commission has not developed emergency plans as required by the Executive Order (pages 15-16); and
- The Commission has not implemented a self-inspection program to provide oversight and individual offices' document control plans were inadequate or out-of-date (pages 16-17).

Based on the above findings, we recommend that the Director of Administration:

- Institute new procedures on issuing identification badges (page 4);
- Implement various controls over physical security addressing combinations, accountability, and destruction of classified documents (page 8);
- Adopt the use of standard forms prescribed for national security information (page 11);
- Familiarize Commission employees with current guidance on classification (page 12);
- Evaluate and revise the security education program (page 15);
- Develop an emergency plan in cooperation with the Information Security Committee (page 16);
- Improve oversight of the Commission's information security program by developing and implementing a self-inspection program and revising Commission policies on information security (page 17).

The Director, Office of Administration agreed with our findings and recommendations, and has already started to take appropriate actions. His comments are discussed in more detail on pages 5, 9, 11, 12, 15, 16 and 17, and presented in their entirety as an Appendix to this report.

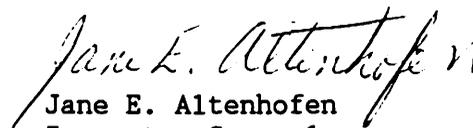

Jane E. Altenhofen
Inspector General

TABLE OF CONTENTS

INTRODUCTION AND SCOPE	1
BACKGROUND	2
FINDINGS AND RECOMMENDATIONS	3
ACCESS	4
Recommendation	4
Commission Comments	5
PHYSICAL SECURITY	5
Combinations	5
Accountability	6
Log	6
Inventory	7
Transmittal	7
Disposition and Destruction	7
Recommendations	8
Commission Comments	9
STANDARD FORMS	9
SF 312 & 189: Classified Information Nondisclosure Agreement	9
SF 700: Security Container Information	9
SF 701: Activity Security Checklist	10
SF 702: Security Container Check Sheet	10
SF 703: TOP SECRET Cover Sheet	10
SF 704: SECRET Cover Sheet	10
SF 705: CONFIDENTIAL Cover Sheet	10
Recommendation	11
Commission Comments	11
CLASSIFICATION	11
Recommendation	12
Commission Comments	12
SECURITY EDUCATION PROGRAM	12
Briefings	13
Initial Briefings	13
Refresher Briefings	13
Termination Briefings	14
Hostile Threat	14
Foreign Travel	14
Recommendations	15
Commission Comments	15
EMERGENCY PLANNING	15
Recommendation	16
Commission Comments	16

OVERSIGHT	16
Self-Inspection Program	16
Document Control Plans	17
Recommendations	17
Commission Comments	17

**Appendix - Memorandum from Director, Office of Administration, dated
September 26, 1990, on Draft Report**

INTRODUCTION AND SCOPE

The Office of Inspector General (OIG) has completed a review of the Commission's information security program. This review was scheduled to coincide with a review performed by the Information Security Oversight Office (ISOO) of the General Services Administration. The objective of this review was to evaluate the Commission's compliance with Executive Order 12356, National Security Information, and the implementing directives issued by the National Security Council (NSC) and ISOO.

Our review was conducted in May through July 1990. The review was performed at Commission headquarters in Washington, D.C. in the Offices of Administration, Executive and International Liaison (XL), General Counsel (GC), the Secretary (SE), and the Agriculture, Fisheries, and Forest Products (AG) and Energy and Chemical (E&C) Divisions in the Office of Industries (IND). We interviewed office representatives to determine policies and procedures concerning the receipt, storage, transmission and destruction of classified material. As part of the office reviews, we traced a sample of Secret documents selected from the 1990 inventory to observe whether they were properly stored and marked.

This review focused on controls over National Security Information (NSI) classified as Confidential or Secret. Most NSI at the Commission is generated or obtained in connection with the preparation of Section 332 reports and classified at the Confidential level. The Commission has no Top Secret information or Special Access Programs.

The Commission policy is for all employees (including temporaries and summer help) to have Secret security clearances. The Commissioners and three Commission staff members have Top Secret security clearances. We reviewed policies and procedures concerning Commission employees and visitors, such as issuing security clearances and badges. We specifically reviewed whether employees had signed non-disclosure agreements and attended security briefings.

We reviewed reports issued by ISOO and the National Security Agency (NSA) on the Commission's security programs. The ISOO reports, issued in September 1987 and July 1990, included the results of their inspections conducted as part of their oversight responsibilities. The NSA report was done in response to the Commission's request for them to conduct a review ascertaining whether the Local Area Network could be certified to store and transmit classified information. We also reviewed the General Accounting Office report "INTERNATIONAL TRADE Observations on the Operations of the International Trade Commission" (GAO/NSIAD-87-80), issued in February 1987, which included items related to NSI.

This review was performed in accordance with generally accepted government auditing standards. Accordingly, the review included an examination of internal controls and other auditing procedures that were considered necessary under the circumstances.

BACKGROUND

Executive Order 12356, issued in April 1982, requires each Federal agency to designate a senior agency official to direct and administer its information security program. The Chairman has designated the Director of Administration as the Commission's security officer. The Director of Administration is responsible for the implementation and oversight of information security programs and procedures in the Commission, including ensuring conformity with the provisions of the Executive Order.

The Commission also has an Information Security Committee (ISC) which is responsible for implementing and overseeing information security programs and procedures, acting on all questions, suggestions, and complaints with respect to the Commission's administration of the program; and establishing a program for employee education and awareness.

The Executive Order charges the NSC with responsibility for providing overall policy direction and ISOO with responsibility for ensuring effective implementation of the Executive Order. With NSC approval, ISOO issued regulations in June 1982 that include guidance on derivative classification, safeguarding, security education and oversight. The NSC issued National Security Decision Directive 197, Reporting Hostile Contacts and Security Awareness, in November 1985, that requires each agency to create and maintain a formalized security education program addressing foreign contacts.

Commission guidance related to NSI is included in the following Directives:

<u>No.</u>	<u>Date</u>	<u>Subject</u>
1301	06/23/77	Changing Safe Combinations
1303	11/21/84	Personnel Security (National) Program
1305	04/24/90	Improved Physical Security at the USITC
1350	01/25/84	National Security Information (under revision)

In addition, a draft Directive 1304 on Security Container Combinations for Storage of NSI was prepared in August 1987. Directive 1345, Information Security Program, was issued on July 31, 1990. Our field work was completed by that time, but we did consider the Directive in preparing the draft report.

Directive 1350 provides that Office Directors are responsible for reviewing this Directive with their employees annually and sending a certification to the Director of Administration. Office Directors have never been requested to review the Directive with their employees. This requirement has been superseded by a centralized security education program instituted by the Office of Administration.

As required, the Commission issued regulations implementing the Executive Order and ISOO Directive (19 CFR Ch II Subpart F). The regulations include a section on mandatory declassification and state that suggestions or complaints regarding the agency's information security program should be submitted to the Director of Administration.

FINDINGS AND RECOMMENDATIONS

The Executive Order provides that each agency should establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

We found that the Commission has developed an information security program with policies and procedures generally consistent with the Executive Order and implementing ISOO regulations. In some instances, compliance with the policies and procedures is substantial, as in using proper security containers and signing Nondisclosure Agreements.

However, we identified multiple areas where policies and procedures need to be refined and compliance increased in order to fully comply with the provisions of the Executive Order and ISOO regulations. Our findings in these areas are:

- The Commission issues the same type of identification (ID) badges to individuals with and without security clearances;
- Physical security included weaknesses such as: the primary control to ensure combinations were changed as required did not clearly include all security containers, combinations were being changed by locksmiths without security clearances, offices generally did not use an accountability log to control NSI, the annual inventory did not include responses from all offices or all required categories of NSI, inadequate controls over burn bags, particularly that they were being given to a contractor without a security clearance, and that records were not maintained on destruction of Secret documents;
- Confidential reports and workpapers were not marked in accordance with current guidance;
- Some of the standard forms for document security were used sporadically;
- The Security Education Program does not include termination or foreign travel briefings, and the refresher briefing was last offered over a year ago and not attended by all employees;
- The Commission has not developed emergency plans as required; and
- The Commission has not implemented a self-inspection program to provide oversight and individual offices' document control plans are inadequate or out-of-date.

ACCESS

The Executive Order provides that agencies that handle classified information shall establish procedures to prevent unnecessary access to classified information. We found that the Commission issues the same type of ID badge to individuals with and without security clearance. We believe this creates a potential situation for disclosure of NSI to unauthorized persons.

Each Commission employee is given a photo ID badge within one or two days of reporting for duty. All temporary and permanent employees, as well as a few non-Commission employees, are given the same type of ID badge. Employees do not need to show evidence of their security clearance prior to being given the ID badge.

The Commission's ID badge does not connote a security clearance, as it does at some agencies. However, we found that employees do make this association since it is commonly believed that all employees have Secret security clearances and only employees have ID badges.

While it is generally true that only employees with security clearances have ID badges, there are some exceptions. The ID badges are issued immediately, whereas the security clearances may not be processed for several days; the employee does not have a clearance during this period. In a few cases, ID badges have been issued to individuals without security clearances who need long-term access to the Commission. In addition, the preliminary investigations of a few employees indicated further review was warranted and the officials involved agreed to restrict access by these employees to NSI until the reviews were completed.

The Office of Management Services (OMS) said employees want the ID badge immediately so they do not have to sign in and out and the expense and time would be prohibitive to issue two ID badges to each new employee. However, the Commission has temporary passes that can be issued for a period of time. These are basically the paper visitor passes in a plastic case and do not have a picture of the individual. There would be minimal cost or time involved in issuing these passes and the regular ID badge could be issued as soon as the employee received a security clearance.

As for long-term visitors and employees without a full Secret clearance, alternative IDs should be provided to avoid any appearance that they may have access to NSI. OMS is considering buying ID badges that look different from the regular ID badges, but still have a picture, that would be used in these circumstances.

Recommendation

We recommend that the Director of Administration institute procedures whereby temporary passes are given to new employees until they receive notification of their security clearance and alternative ID badges are given to individuals other than employees with full security clearances.

Commission Comments

The Director of Administration has agreed with the recommendation. He stated that it is important to change the procedures if employees are making the association between ID cards and security clearances even though the issuance of ID cards was not supposed to be connected with the security clearance procedure.

PHYSICAL SECURITY

ISOO regulations state that classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it. We found all Secret documents were properly stored and that employees either had in their offices or had access to proper security containers for storage of Confidential documents.

We also found several weaknesses in physical security. The primary control to ensure combinations were changed as required did not clearly include all security containers and combinations were being changed by locksmiths without security clearances. Offices generally did not use an accountability log to control NSI and the annual inventory did not include responses from all offices or all required categories of NSI. We observed inadequate controls over burn bags, particularly that they were being given to a contractor without a security clearance, and that records were not maintained on destruction of secret documents.

Combinations

ISOO regulations state that combinations to dial-type locks shall be changed only by persons having an appropriate security clearance and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to it, whenever a combination has been subjected to possible compromise, whenever the equipment is taken out of service, or at least once every year. Directive 1301 states that offices are responsible for changing safe combinations in the above listed conditions and, whenever a combination is changed, a copy of the new combination should be placed in a sealed envelope and placed in the Secretary's safe.

Although he is not assigned any responsibility to monitor changes of combinations, the Secretary had developed a list of offices with security containers and notified the offices when a year had passed that it was time to change the combination. Each office we reviewed was aware that the Secretary maintained a list of security containers and relied on this control. This control technique is not totally effective because all security containers may not be on the list.

The Secretary derived the list based on receipt of envelopes from offices notifying him that the combination had been changed and a list of safes from the OMS property list. There are several weaknesses in this process. First,

the Commission Directives do not require that the Secretary be notified of new security containers, only of changes in combinations. Directive 1301 refers only to safes, so it is unclear whether the Secretary's responsibilities apply to just safes or all security containers (safes and certain file cabinets), and whether the requirement is for containers that could contain NSI, or only the ones that actually store NSI.

Furthermore, the Secretary cannot tell from the notification the type or number of security containers in each room. He does not open the envelopes (in accordance with Directive 1301) so he can only list the room and individuals with access if they are identified on the envelope.

We believe that the procedural problems of this control technique result at least partially because this is an ad hoc responsibility of the Secretary. The Directives only require that the Secretary be a repository for combinations. The Office Directors have responsibility for ensuring that combinations are changed as appropriate. The Secretary assumed this responsibility some years ago, yet it has never been set forth in a Directive with the accompanying procedures.

ISOO regulations (32 CFR 2001.43(b)(1)) state that combinations to dial-type locks shall be changed only by persons having an appropriate security clearance. The regulations do not include a provision for waiving this requirement. OMS uses locksmiths who do not have security clearances to change combinations. OMS has adopted procedures stating that locksmiths are to be accompanied at all times by an employee with a Secret security clearance.

Accountability

Two major controls over accountability of NSI are the use of a log and annual inventories. We found that offices generally did not use an accountability log to control NSI and the annual inventory did not include responses from all offices or all required categories of NSI.

Log

Accountability was an issue in the GAO report and in the ISOO reviews. The 1987 ISOO report said accountability had been improved because the Commission was developing an accountability log for controlling classified information. The 1990 ISOO report stated that the ITC had implemented a new document accountability form entitled "National Security Information Log".

The Office of Administration could not locate a memorandum instructing offices to use this log. Only one of the offices we visited, the Secretary, used the log. The other offices did not use it or remember seeing a recent memorandum distributing the log. Some offices used the inventory from the prior year and simply added new documents to the list. The OGC did not maintain a list - documents were kept in separate sealed envelopes, for each attorney, in the safe.

Inventory

The ISOO regulation states that an inventory of Top Secret documents shall be made at least annually and agency heads shall prescribe control requirements for Secret and Confidential information. Directive 1350 states that each office will maintain a record of receipt and disposition of Top Secret, Secret, and all Confidential documents marked with special dissemination instructions/restrictions. In January of each year, an inventory is to be filed with the Director of Administration.

An inventory of Secret and Top Secret documents was taken in early 1989 and 1990. The 1990 inventory did not request that offices identify Confidential documents with special instructions/restrictions and a response was not on file from two offices (neither of which had Secret or Top Secret documents at the time of our review). The Office of Administration said that the inventory request had included the specified Confidential documents at one time, and could be reinstated if this requirement is maintained in the revised Directive 1350.

The five offices we visited had a large majority of all the Secret documents listed in the 1990 inventory. Since the documents were kept in one drawer, and often one file, we verified virtually all of these documents as being on hand.

Transmittal

ISOO regulations provide detailed instructions on the wrapping and receipting and transmittal methods for NSI. The Commission Directives are in accordance with this guidance. Information transmitted outside the agency is usually hand carried.

Disposition and Destruction

ISOO regulations state that classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude recognition or reconstruction of the classified information or material. Directive 1350 states that Secret and Confidential documents will be destroyed by shredding.

The Commission has several shredders throughout the agency on which NSI can be shredded. More commonly, employees put NSI in burn bags for destruction. The burn bags are stored in room 119-A or a secure storage area in the Navy Yard. Some of the documents in burn bags are shredded in a large machine located in the Print Shop by Commission staff, but most are shredded by a contractor.

Directive 1350 states that burn bags en route to the shredder are still classified and must be given the appropriate level of protection. Burn bags will not be left unsecured or unattended.

Office representatives said, and we observed, that burn bags were usually kept in the open area by the support staff waiting to be picked-up by the mail staff. Some individuals said they kept open burn bags by their desks, and secured at night, until they were full for pick-up. We accompanied mail room employees on four runs to pick up burn bags and on two occasions burn bags were in rooms unattended.

More significantly, the contractor who picks-up the documents for shredding at its facility does not have a security clearance. OMS said that the contractor only destroys sensitive and confidential business information. NSI is put in specially marked burn bags and shredded in-house. The Directives do not mention marking burn bags as containing NSI nor did any employees mention this distinction.

Directive 1350 also requires that offices annotate the date and method of destruction of all Secret and Confidential documents with special dissemination restrictions in the Office records. The Office of International and Executive Liaison was the only office we visited that had destroyed Secret documents within the past year. The staff assistant shredded these documents and did not keep a record of the date or method of destruction.

Recommendations

We recommend that the Director of Administration:

1. Determine whether the Secretary should have responsibility for ensuring that locks are changed when appropriate and if so, develop implementing procedures;
2. Ensure locks are changed by individuals with security clearances or obtain a waiver from ISOO for this requirement;
3. Notify offices that they are to use the "National Security Information Log";
4. Clarify inventory policy and procedures regarding Confidential documents with special access instructions/restrictions and ensure all offices are included in the inventory;
5. Take immediate steps to ensure that NSI is not given to a contractor for destruction until ISOO is consulted; and
6. Ensure offices are familiar with the instructions on the content of burn bags and proper security measures and know the recordkeeping requirements for the destruction of documents.

Commission Comments

The Director of Administration agreed to take the recommended steps to improve physical security. He immediately discontinued the practice of sending NSI to a contractor for destruction upon learning that the contractor did not have a current clearance.

STANDARD FORMS

ISOO regulations state that the use of standard forms (SF) prescribed in the regulations is mandatory. ISOO's 1987 report stated that the Commission had implemented procedures for using the standard forms. The Commission Directives only specifically address using the SF 312/189.

As discussed in the following sections, we found a few of the forms were used consistently, but the others were used sporadically. The ISOO regulations provide that the NSC or ISOO may approve a waiver to using the forms, but the Commission has not requested such a waiver.

SF 312 & 189: Classified Information Nondisclosure Agreement

All employees of independent agencies must sign an Agreement (SF 189 until replaced by the SF 312) prior to being given access to NSI. The completed Agreements must be retained in a file system that will assure their recovery for a period of 50 years.

As set forth in Directive 1350, the Office of the Secretary is responsible for maintaining such files. The Secretary ensures that all new employees sign Agreements which are kept in the personnel security files. We selected a sample of 20 employees from the April 1990 telephone directory. Agreements were on file for all of them. The Secretary knew that the Agreements had to be maintained for 50 years. He had files for Agreements signed since 1984, which is when they were first used.

SF 700: Security Container Information

This form provides the names, addresses and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended. The form also includes the means to maintain a current record of the security container's combination. The form is to be attached to the inside of the container and a copy sent to a designated party for safekeeping.

The Commission established procedures for the use of SF 700 in the draft Directive 1304 circulated in October 1987 (this guidance was never finalized). The draft Directive states that combinations for all containers containing NSI must be recorded on SF 700 with a copy delivered to the Office of the

Secretary. Sometime within the last year, the Secretary began requesting that offices use SF 700 when reporting the change in combinations as required in Directive 1301.

Two offices we visited used this form, the Secretary and Executive and International Liaison. The OGC and two divisions in the Office of Industries did not use the form and were not aware that they were supposed to use it.

We opened two of the sealed envelopes sent to the Secretary. Both were literally scraps of paper, neither had a name, one had a two-digit combination and one had a four-digit combination listed (three-digits are correct). This type of information would not be very helpful either if the combination was forgotten or the safe was left open.

SF 701: Activity Security Checklist

This form provides a systematic means to make a thorough end-of-day security inspection for a particular work area. Directive 1350 states that the head of each office or division having custody of NSI will take the necessary actions to ensure that subordinate managers and supervisors conduct a security check at the end of each work day. A log of daily security checks (not specifically SF 701) shall be maintained. The 1987 ISOO report said that the Commission had implemented procedures for using ISOO's standard forms for end-of-day security checks. The Office of Administration said Office Directors had been instructed to develop office policies for using this form.

We found the offices had established varying policies on the use of this form and the policies were followed in varying levels:

<u>Office</u>	<u>Policy</u>	<u>Practice</u>
OGC	none	not used
IND	every office	Agric. used predominantly E&C used sporadically
Sect	office-wide check	used consistently
EX	office-wide check	used consistently

SF 702: Security Container Check Sheet

This form provides a record of the names and times that persons have opened, closed or checked a particular container that holds NSI. Commission Directives do not refer to this form. We found the forms and signs were on all containers with NSI and used appropriately.

SF 703: TOP SECRET Cover Sheet

SF 704: SECRET Cover Sheet

SF 705: CONFIDENTIAL Cover Sheet

These forms serve as a shield to protect NSI from inadvertent disclosure and to alert observers that NSI is attached. Commission Directives do not refer to these forms. While verifying that Secret documents listed in the 1990 inventory were on file, we observed that none of the offices had cover sheets on the documents. While reviewing Confidential documents, we observed a few individual documents or files had cover sheets, but many documents did not have the forms.

Recommendation

We recommend that the Director of Administration notify all offices that the standard forms are to be used and incorporate these requirements into the revised instruction.

Commission Comments

The Director of Administration agreed to include specific instructions on the use of all the standard forms prescribed by Executive Order 12356 in the revised Directive 1350.

CLASSIFICATION

Although the Commission does not have original classification authority, employees do mark documents in accordance with classification instructions provided by the USTR. We found that reports and workpapers were not marked in accordance with current guidance.

Since 1982, the Commission had been working under guidance that all reports requested from USTR were to be classified Confidential. The ISOO 1987 report stated that deficiencies in the USTR guidance resulted in the Commission not correctly marking the reports. The Office of Administration coordinated with the USTR and ISOO to obtain guidance, which was provided on February 16, 1989. Based on ISOO's comments, this guidance was slightly amended on August 25, 1989. The Commission and senior staff were notified of this guidance on September 13, 1989.

The guidance primarily addresses marking the reports. The cover should include the following statements:

CLASSIFIED BY: The Office of the United States Trade Representative, in accordance with guidance letter dated February 16, 1989.

DECLASSIFY ON: Originating Agency Determination Required (OADR)

During meetings with employees in the Office of Industries, we found the wording was wrong in both of these sections in two final reports. We then reviewed eight Confidential reports issued by the Office of Industries in 1990

and found all of them were incorrectly marked. All but two documents were marked in accordance with the February 16 guidance which had been superseded. The other two documents cited the letter requesting the report rather than the classification guidance letter.

USTR guidance also states that "Confidential" must be marked on the top and bottom of the front cover, back cover (outside), title page, and first page. The top and bottom of each page must be marked with either the highest classification of the content of the page, or the overall classification of the report. We found that the final reports were generally marked in accordance with this guidance. Two reports had attachments not marked as confidential or unclassified.

USTR guidance states that workpapers that are so far advanced that they reveal USITC findings, opinions or recommendations should also be classified at the Confidential level. This is a difficult policy to implement because the guidance is not very precise, but we believe it certainly includes draft reports. We observed that a draft section of a pre-hearing report was not classified at all and another pre-hearing report was only marked Confidential on the first page rather than each page as required.

Recommendation

We recommend that the Director of Administration ensure that Office Directors are familiar with current USTR guidance and have provided instructions to their employees.

Commission Comments

The Director of Administration agreed with this recommendation. The Director of Industries, the primary office involved in marking documents, has already issued additional instructions to its divisions. The guidance provided by USTR will also be included in the revised Directive 1350.

SECURITY EDUCATION PROGRAM

ISOO regulations prescribe that each Federal agency that creates or handles NSI must establish a security education program sufficient to familiarize all necessary personnel with the provisions of the Executive Order and its implementing directives and regulations and to impress upon them their individual security responsibilities.

We found that the Commission provides initial and refresher briefings, but not termination briefings. Furthermore, the refresher briefing was last offered over a year ago and was not attended by all employees. The Commission has presented a hostile threat briefing which must be done periodically. The Commission does not give foreign travel briefings.

Briefings

ISOO regulations require that security education programs provide initial, refresher and termination briefings. We found that the Commission provides initial and refresher briefings, but not termination briefings. Furthermore, the refresher briefing was last offered over a year ago and was not attended by all personnel.

Initial Briefings

The initial briefing consists of having the employees sign the SF 312 (previously the 189) and providing them copies of Directives 1350, 1355, and 1360. The Commission also schedules quarterly briefings for new employees. These were last held in February, August, and December 1988 and June 1989. New employees were strongly encouraged to attend these briefings, and most did attend.

Briefings have not been scheduled for the last year pending an update of the briefing slides.

Refresher Briefings

Each employee is to attend an annual refresher briefing arranged by the Office of Administration, regardless of whether a quarterly initiation briefing had been attended within the previous year. The refresher briefing was last offered in April and May, 1989.

We found 92 employees did not attend any of the April or May sessions. 51 attended a quarterly meeting scheduled in June. The remaining 41 employees were in the following offices:

	Employed as of 6/30/89	Employed as of 6/30/90
Commissioners	2	1
GC	5	3
PN	1	
OUII	1	1
ODS	3	
OMS	1	
PA	1	
ADM	2	1
IND	8	4
TATA	1	1
Econ	9	4
XL	1	1
INV	6	5

Furthermore, 5 of the 41 employees did not attend a briefing in 1988 either. Two of these employees were at the Commission as of June 1990, although one of these left in mid-July. The one individual who has not

attended is in one of the offices with the most NSI (XL) and has gone so far as to sign the roster at the June 1990 briefing but leave before hearing the presentation.

We believe the Office of Administration has fulfilled their responsibilities by scheduling a series of the refresher briefings, notifying the Office Directors that attendance is mandatory, and recording who has attended the briefings. The process concerning refresher briefings needs to be rethought to lessen the burden on the Office of Administration and place more responsibility on the Office Directors and the employees themselves.

Refresher briefings have not been scheduled for the last year pending an update of the briefing slides.

Termination Briefings

The 1987 ISOO report stated that employees leaving the Commission are orally briefed on their continuing responsibility to protect classified information to which they had access and to return any classified material. The Office of Administration said that the employee discharge list requires a sign-off from the supervisor that all classified material has been returned, but supervisors have not been instructed to debrief employees. There is a space on the SF 312 for a security debriefing acknowledgement but it is not used either.

Hostile Threat

National Security Decision Directive 197, Reporting Hostile Contacts and Security Awareness, November 1985, requires each agency to create and maintain a formalized security education program addressing foreign contacts. The program must include periodic formal briefings of the threats posed by hostile intelligence services.

The Commission presented a briefing on this topic in 1988. A future briefing on this topic has not been scheduled.

Foreign Travel

The 1987 ISOO report suggested that the Commission consider offering foreign travel briefings. The Commission and employees regularly travel overseas and have contacts with local officials in the course of business so foreign travel briefings are appropriate.

The Office of Administration is considering how to implement this suggestion. One fairly simple method would be to distribute a pamphlet on security for foreign travel with the signed authorization for overseas travel.

Recommendations

We recommend that the Director of Administration:

1. Resume giving refresher briefings within the next quarter;
2. Revise procedures so that the ultimate responsibility for attending security briefings is given to the Office Directors and the employees;
3. Implement termination briefings;
4. Establish a policy on providing periodic briefings on hostile threat;
5. Evaluate the benefits of providing foreign travel briefings and implement if appropriate.

Commission Comments

The Director of Administration agreed with these recommendations. Annual briefings were held for all employees on August 29 and 30, 1990, and an alternative briefing method was made available for those who could not attend. The Commissioners and Office Directors were given the responsibility to certify that their employees either attended the briefing or read and understood the security materials provided. The requirement for termination briefings and provisions for materials or briefings on foreign travel and hostile threat will be included in the revised Directive 1350.

EMERGENCY PLANNING

The ISOO regulation states that agencies shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. The Commission has not developed any such plans.

The Secretary had suggested to the Chairman in 1987 that a committee be formed to address Emergency Response Planning. His memorandum cited the following emergencies that had occurred - a fire in the ITC building, a riot in the neighborhood, severe weather, structural damage to the building, a mail strike, and a city-wide power shortage.

The memorandum was referred to the Director of Administration for information, but no direction to take action was given.

Recommendation

We recommend that the Director of Administration in cooperation with the ISC develop an emergency plan for protecting classified material.

Commission Comments

The Director of Administration agreed with this recommendation. The plan will be included in the revised Directive 1350.

OVERSIGHT

ISOO regulations state that agency heads shall require that periodic formal reviews be made to ensure compliance with the provisions of the Executive Order and ISOO directives. The Commission has not implemented a self-inspection program to provide oversight. Individual offices did develop document control plans to safeguard information, but these are inadequate or out-of-date.

Self-Inspection Program

The 1987 ISOO report recommended that the Commission establish a formal self-inspection program that, as a minimum, would include procedures to ensure that accountability practices are being followed, required inventories are being conducted, the security education program is informative and current, and provide for a periodic and routine review of samples of NSI.

The Commission intended to implement a self-inspection program. The 1987 internal control review for information security identified a control technique for the Periodic Security Checks Cycle to "on an irregular schedule conduct an inspection of the offices procedures for handling, storage, recording marking destruction of classified information and confidential business information, with the findings reported to the Information Security Committee". However, this control was not implemented.

The 1990 ISOO report noted that the self-inspection program had not yet been implemented, but was provided for in the revised Directive to be issued in July 1990 (the current estimate is for the draft Directive to be issued in August 1990 and the final some time thereafter). The ISOO report further stated that the Commission conducted on-the-spot security checks. An Office of Administration representative said that ISOO may have misinterpreted a discussion on how the Office of Administration follows-up on any infractions identified.

Document Control Plans

Directive 1350 states that document control plans specifying procedures appropriate for safeguarding NSI will be developed by the ISC (with input from Office Directors as appropriate) and reviewed annually. Plans were developed by the individual offices in 1987 and submitted to the ISC for review.

We reviewed the plans for the Offices of Industries, GC, XL and Secretary. Several of the plans were too brief to ever have been of much use and the others are now out-of-date. For instance, the GC plan states that they will keep all NSI in the Secretary's safe. The plan was not revised to reflect current procedures when they began to store NSI in the office safe.

A difficulty in updating the office policies is that the Commission-wide policies need to be consolidated and updated. The multiple directives and memorandums on information security are confusing and in some aspects obsolete and/or contradictory. Once the Commission policies are established, office policies can be established that address how to specifically implement the Commission policies. For instance, office policies would establish whether the Activity Security Checklist would be done on an office-wide or individual office basis and where burn bags would be kept for pick-up.

Recommendations

We recommend that the Director of Administration:

1. Develop and implement a self-inspection program; and
2. Complete the revision of the Commission policies on information security and thereafter, if appropriate, request that Office Directors submit updated document control plans for review by the ISC.

Commission Comments

The Director of Administration agreed with this recommendation. He will assess whether the self-inspection program, which will be included in the revised Directive 1350, has sufficient controls so that individual office document control plans are not needed.



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

September 26, 1990

MEMORANDUM

TO: Inspector General

FROM: Director, Office of Administration *L. M. L. Goodrich*

SUBJECT: Draft Report, "Review of USITC's Information Security Program"

As requested by your memoranda dated August 14, 1990 and August 30, 1990, (IG-N-088 and IG-N-094), submitted as an attachment to this memorandum is the Office of Administration's response to the subject draft audit report issued on August 1990. In accordance with Section 11 of the USITC Directive 1701, the Commissioners have had an opportunity to comment on the response and the Chairman has approved it.

Please call me at 252-1131 or Bill Stuchbery at 252-1135 if you have any questions.

Attachment

cc: Secretary
General Counsel
Director, Office of Investigations
Director, Office of Industries
Director, Office of Economics
Director, Office of Executive and International Liaison
Director, Office of Management Services
Director, Office of Information Resources Management

September 11, 1990

OFFICE OF ADMINISTRATION'S RESPONSE TO THE AUGUST 1990
DRAFT AUDIT REPORT ON THE REVIEW OF USITC'S
INFORMATION SECURITY PROGRAM

FINDINGS AND RECOMMENDATIONS

ACCESS

The Commission issues the same type of identification (ID) badges to individuals with and without security clearances.

RECOMMENDATION:

We recommend that the Director of Administration institute procedures whereby temporary passes are given to new employees until they receive notification of their security clearance and alternative ID badges are given to individuals other than employees with full security clearances.

AGREE: We agree with your recommendation that temporary passes be issued to new employees until they receive their security notification. In addition, alternative badges will be given to those people who do not require a security clearance. We feel it is important to change the procedures if employees are making the association between ID cards and security clearances. The issuance of ID badges in the Commission has not been connected with the security clearance procedure. The supervisors of the new employees are given the clearance notification by the Personnel Security Officer. This has been the method of determining when an employee is cleared and when they could be assigned duties which require the handling of classified material.

COMPLETION DATE: December 31, 1990

PHYSICAL SECURITY

Physical security included weaknesses such as: the primary control to ensure combinations were changed as required did not clearly include all security containers, combinations were being changed by locksmiths without security clearances, offices generally did not use an accountability log to control NSI, the annual inventory did not include responses from all offices or all required categories of NSI, inadequate controls over burn bags, particularly the ones that are being given to a contractor without a security clearance, and that records were not maintained on destruction of Secret documents.

RECOMMENDATIONS:Combinations

1. Determine whether the Secretary should have responsibility for ensuring that locks are changed when appropriate and if so, develop implementing procedures.

AGREE: We plan to cancel Directive 1301, Changing Safe Combinations, and issue Directive 1304, Security Containers Combinations for Storage of National Security Information which will provide the necessary procedures and areas of responsibility.

COMPLETION DATE: January 31, 1991

2. Ensure locks are changed by individuals with security clearances or obtain a waiver from ISOO for this requirement;

AGREE: The Office of Management Services (OMS) has already begun the process of obtaining the necessary certification of a locksmith services vendor. Until certification can be obtained, OMS will continue its current practice of escorting the locksmith when such services are required.

COMPLETION DATE: March 31, 1991

Accountability

3. Notify offices that they are to use the "National Security Information Log".

AGREE: We intend to revise Directive 1350 to include specific instruction on the use of the national security information log sheet.

COMPLETION DATE: April 30, 1991

4. Clarify inventory policy and procedures regarding Confidential documents with special access instructions/restrictions and ensure all offices are included in the inventory.

AGREE: We intend to revise Directive 1350 to comply with the ISSO's regulations concerning inventory and eliminate the term "confidential documents with special dissemination instructions/restrictions". The Office of Congressional Liaison and the Office of Inspector General will be included in the next NSI inventory.

COMPLETION DATE: April 30, 1991

5. Take immediate steps to ensure that NSI is not given to a contractor for destruction until ISOO is consulted.

AGREE: At the time the Inspector General notified us of the situation we discontinued the practice of sending NSI to a contractor for destruction. On August 23, 1990, a letter was sent to the DOD, Defense Industrial Security Program Office (DISP) requesting a facility clearance for a contractor to transport, store and destroy NSI up to and including Secret. The contractor is required to follow the procedures established by DISP.

ESTIMATED COMPLETION DATE: October 31, 1990

6. Ensure offices are familiar with the instructions on the content of burn bags and proper security measures and know the recordkeeping requirements for the destruction of documents.

AGREE: Immediately following notification from the Defense Industrial Security Program Office of the contractors clearance and their procedures, we will issue an administrative notice to Directive 1350. This notice will provide the offices with the procedures and recordkeeping requirements for the destruction of documents.

ESTIMATED COMPLETION DATE: November 15, 1990

CLASSIFICATION

Confidential reports and workpapers were not marked in accordance with current guidance.

RECOMMENDATION:

We recommend that the Director of Administration ensure that Office Directors are familiar with current USTR guidance and have provided instructions to their employees.

AGREE: As indicated in the Inspector General's report the Commission and senior staff were notified on September 13, 1989 of the most recent guidance from USTR by the Chairman. Following your interview with the Office of Industries, that office issued additional instructions to its divisions guidance provided by USTR on August 25, 1989. This included the clarification regarding the classification of "working papers", and revised guidance on marking the front covers of the reports with classification/declassification instructions (a copy is attached). The guidance provided by USTR will be included in the revised Directive 1350.

COMPLETION DATE: April 30, 1991

STANDARD FORMS

Some of the standard forms for document security were used sporadically.

RECOMMENDATION:

We recommend that the Director of Administration notify all offices that the standard forms are to be used and incorporate these requirements into the revised instruction.

AGREE: We intend to revised Directive 1350 to include specific instruction on the use of all the standard forms prescribed by Executive Order 12356.

COMPLETION DATE: April 30, 1991

SECURITY EDUCATION PROGRAM

The Security Education Program does not include termination or foreign travel briefings, and the refresher briefing was last offered over a year ago and not attended by all employees.

RECOMMENDATIONS:

1. Resume giving refresher briefings within the next quarter.
2. Revise procedures so that the ultimate responsibility for attending security briefings is given to the Office Directors and the employees.
3. Implement termination briefings.
4. Establish a policy on providing periodic briefings on hostile threat.
5. Evaluate the benefits of providing foreign travel briefings and implement if appropriate.

AGREE: On August 29 and 30, 1990 the annual briefings were held for all employees. In addition, starting this year, we also made available an alternative briefing method for those who were unable to attend. It is now the responsibility of the Commissioners and Office Directors to certify that their employees have either, attended the briefing or read and understand the security materials provided.

In revising Directive 1350 we will include the requirement for termination briefings, and in the security awareness section provisions for materials or briefings on foreign travel and hostile threat.

COMPLETION DATE: April 30, 1991

EMERGENCY PLANNING

The Commission has not developed emergency plans as required.

RECOMMENDATION:

We recommend that the Director of Administration in cooperation with the

ISC develop an emergency plan for protecting classified material.

AGREE: The Office of Administration will coordinate with the Information Security Committee the development of a plan for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. This plan will be included in the revised Directive 1350.

COMPLETION DATE: April 30, 1991

OVERSIGHT

The Commission has not implemented a self-inspection program to provide oversight and individual offices' document control plans are inadequate or out-of-date.

RECOMMENDATIONS:

1. Develop and implement a self-inspection program; and
2. Complete the revision of the Commission policies on information security and thereafter, if appropriate, request that Office Directors submit updated document control plans for review by the ISC.

AGREE: In the draft revised Directive 1350 we plan to recommend a self-inspection program. As a result of the numerous controls to be implemented in the revised Directive 1350, there may not be the need for individual office to maintain document control plans. This can be determined during the review of the draft directive.

COMPLETION DATE: April 30, 1991

TECHNICAL CORRECTIONS

Page 1, fourth paragraph. The draft report is not correct regarding employees with Top Secret clearances. If we are dealing with ITC staff only, we have three people with Top Secret clearances.

Director, Office of Executive Liaison
Director, Office of Administration
Secretary

If you include all personnel at the agency, the correct number is currently seven (the three listed above, plus four Commissioners).



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

August 20, 1990

MEMORANDUM

TO: Division Chiefs

FROM: Director, Office of Industries *Robert A. Rogojensky*

SUBJECT: Classification Guidance from USTR

On February 16, 1989, the USTR provided classification guidance on reports requested by the President or the USTR (see ID memo dated March 6, 1989 attached). On August 25, 1989, the USTR provided (1) clarification regarding the classification of "working papers" and (2) revised guidance on marking the front covers of our reports with classification/declassification instructions (see attached USTR letter). Inadvertently, the instructions provided in the latter letter have not been implemented at the Commission; the purpose of this memorandum is to institute the new instructions within the Office of Industries.

1. Working papers.--The 2/16/89 USTR letter states--

"None of the reports and working papers classified in accordance with USTR guidance are to be released to the public until a declassification determination is made by my office."

The USTR letter of 8/25/89 defines "working papers" as--

"...papers that are so far advanced that they reveal USITC findings, opinions, or recommendations, including but not limited to drafts of reports and portions of draft reports. In specific circumstances, USTR may wish to classify additional papers gathered or generated by the USITC during an investigation, such as notes from interviews. In those circumstances, USTR will specifically identify the additional papers or class of papers that the Commission should treat as classified....In addition, unless USTR provides otherwise, the USITC should not treat working papers relating only to unclassified sections of a report as classified."

Division Chiefs--Page 2

2. Classification/declassification markings.--Beginning immediately all Confidential reports to the USTR are to have the following, revised classification/declassification instructions on the front cover (in addition to the "CONFIDENTIAL" marking at top and bottom of page--see sample attached):

CLASSIFIED BY: United States Trade Representative, Letter Dated
February 16, 1989

DECLASSIFY ON: Originating Agency Determination Required

The Publishing Division has been notified of this new standard language,
but please check covers before releasing future reports.

Attachment

cc: D/OPS
D/Admin
GC
D/OE
D/TATA
Chf/PD



UNITED STATES INTERNATIONAL TRADE COMMISSION

March 6, 1989

WASHINGTON, D.C. 20436

MEMORANDUM

TO: Division Chiefs

FROM: Acting Director, Office of Industries *Van Dusen*

SUBJECT: New Classification Guidance from USTR

Attached is a letter recently received from the USTR which outlines new classification guidelines for the Confidential 332 reports done for the USTR. The following points seem to be of particular importance:

1. The front cover of the report will have new wording regarding classification authority and declassification instructions. The Publishing Division has already been notified of this new standard language, but please check covers before releasing future reports.
2. Mark "CONFIDENTIAL" at the top and bottom of--
 - a. Front cover
 - b. Back cover (outside)
 - c. Each interior page.
3. For each report requested by USTR, we will provide a draft outline of the report to Bill Hart for transmittal to USTR as soon as possible after the Commission approves the initiating AJ. Based on that outline the USTR will provide us details regarding any further classification specifics for the report in question. Such specifics might include instructions regarding "portion markings." This simply means that certain portions of the report may be classified and other portions may not.

For example, in GSP digests we may be told from the outset that only the probable effects pages will be classified and all other background material will not. In such a case, the Feb. 16 USTR letter seems to offer two options. First, mark each title and subject (and probably each paragraph) with a classification, or second, place a statement at the beginning of the report which identifies the information that is classified as confidential and that which is unclassified. The latter option seems more desirable if it is workable for the study in question; certainly it could work in a digest type format.

Division Chiefs--Page 2

In the event that USTR does not respond to our draft report outline with specific instructions, we are to assume that all portions of the report are classified confidential.

cc: D/XL

THE UNITED STATES TRADE REPRESENTATIVE
Executive Office of the President
Washington, D.C. 20508

Aug 25 1989

OFFICE OF THE CHAIRMAN

SEP 5 12:08

RECEIVED

The Honorable Anne Brunsdale
Chairman
U.S. International Trade Commission
500 E Street, S.W.
Washington, D.C. 20436

Dear Chairman Brunsdale:

On February 16, 1989, I provided the Commission with revised instructions on the confidential classification of certain reports requested by the President, by the USTR on the President's behalf, or by the USTR pursuant to previous authority or pursuant to Executive Order 12661. Pursuant to discussions between our respective staffs, the purpose of this letter is to clarify the treatment of working papers in the preparation of these reports and the applicability of the classification guidance to procedures under Section 22 of the Agricultural Adjustment Act.

As used in my February 16, 1989 letter, the term "working papers" includes papers that are so far advanced that they reveal USITC findings, opinions, or recommendations, including but not limited to drafts of reports and portions of draft reports. In specific circumstances, USTR may wish to classify additional papers gathered or generated by the USITC during an investigation, such as notes from interviews. In those circumstances, USTR will specifically identify the additional papers or class of papers that the Commission should treat as classified.

Section 22 investigations will continue to be subject to the February 16, 1989 procedures, but our expectation is that the classification practice will in general permit the continuation of public briefing and votes by the Commission.

In addition, unless USTR provides otherwise, the USITC should not treat working papers relating only to unclassified sections of a report as classified.

Also, I am enclosing a copy of comments which I have received recently from the Information Security Oversight Office (ISOO) on the classification guidance to the Commission contained in my

The Honorable Anne Brunsdale
Page 2

letter of February 16, 1989. ISOO proposed two modifications in that guidance which will improve ITC's ability to implement our classification instructions and mark documents properly. We have accepted the ISOO proposals, and the guidance with respect to marking instructions is hereby modified accordingly.

Thank you for your careful attention to this matter.

Sincerely,



Carla A. Hills

THE UNITED STATES TRADE REPRESENTATIVE
Executive Office of the President
Washington, D.C. 20508

February 16, 1989

The Honorable Anne E. Brunsdale
Acting Chairman
U.S. International Trade Commission
500 E Street, S. W.
Washington, D. C. 20436

Dear Chairman Brunsdale:

I am writing to revise the U.S. Trade Representative's (USTR) guidance to the U.S. International Trade Commission (USITC) on the confidential classification of certain reports requested by the President, by the USTR on the President's behalf, or by the USTR pursuant to previous authority or pursuant to Executive Order 12661. This letter updates the July 21, 1982 letter from William E. Brock to then USITC Chairman Alfred Eckes.

Under the authority of Executive Order 12356 (the Order), as implemented in 47 FR 20105, all reports prepared by the USITC under section 332 of the Tariff Act of 1930, sections 131 and 503 of the Trade Act of 1974, and section 22 of the Agricultural Adjustment Act are classified confidential. Detailed classification guidance will be provided for each request directed at the Commission.

None of the reports and working papers classified in accordance with USTR guidance are to be released to the public until a declassification determination is made by my office. Any knowing, willful, or negligent disclosure of such classified information will result in sanctions in accordance with section 5.4 of the Order.

Please mark such reports and working papers in the following manner to comply with Executive Order 12356 and Information Security Oversight Office Directive No. 1:

OFFICE OF THE CHAIRMAN

FEB 23 10:01

RECEIVED

1. Designation of Original Classification Authority and Declassification Instructions

Print on the cover of the report the following:

CLASSIFIED BY: The Office of the United States Trade Representative, in accordance with guidance letters dated February 16, 1989 and July 21, 1982.

DECLASSIFICATION INSTRUCTIONS: Upon determination by USTR.

2. Overall Markings

Mark "Confidential" on the top and bottom of the front cover, back cover (outside), title page, and first page.

3. Page Markings

Mark the top and bottom of each interior page with either the highest classification of the content of the page, or the overall classification of the report.

4. Portion Markings

In accordance with specific guidance provided on each requested report, mark each portion of the document, including subjects and titles, by placing a parenthetical designation immediately preceding or following the text to which it applies (i.e., (U) for unclassified, (C) for confidential), or place a statement at the beginning of the report which identifies the information that is classified as confidential and that which is unclassified.

All future requests are subject to this procedure, and should be deemed to be made on the following basis:

In accordance with USTR policy, the USTR has directed that such portions of the Commission's reports and its working papers as identified in a classification guide are classified confidential. Information Security Oversight Office Directive No. 1 (sections 2001.20 and 21, implementing Executive Order 12356 sections 2.1 and 2.2) requires that classification guides identify or categorize the elements of information which require protection. Accordingly, the Commission shall provide the USTR with an outline of each requested report as soon as possible after receipt of the request. Based

The Honorable Anne E. Brunsdale
February 16, 1989
Page 3

on this outline and USTR's knowledge of the information to be covered in the report, a USTR official with original classification authority will provide detailed instructions.

Thank you for your careful attention to this matter.

Sincerely,



Carla A. Hills

CAH:nh



Information Security Oversight Office
Washington, DC 20405



WHS
Call
...

August 16, 1989

Dear Madam Ambassador:

Executive Order 12356, "National Security Information," assigns to the Director of the Information Security Oversight Office (ISOO) the responsibility for monitoring the information security programs of executive branch agencies that generate or handle national security information.

In fulfillment of this responsibility, ISOO reviewed a copy of the United States Trade Representative's (USTR) classification guidance letter dated February 16, 1989, to the International Trade Commission (ITC) regarding the Confidential classification of certain reports requested by the President, the USTR on the President's behalf, or by the USTR pursuant to previous authority or pursuant to E.O. 12661. The review revealed two areas of guidance that, with modification, will improve ITC's ability to classify and mark USTR's information properly.

First, in section one, the "Classified by" line should only reference the latest guidance letter i.e., Classified By: United States Trade Representative, (Letter Dated 02/16/89). This change is necessary because the July 21, 1982 letter, signed by former Trade Representative Brock, cites Executive Order 12065 as its basis for authority. Effective August 1, 1982, Executive Order 12356 implements the current national security information system. Therefore, the current classification guidance letter sent to ITC in February 1989 supersedes the 1982 letter rather than updating it.

USTR letter
7/21/89

End page
reference to both 2/16/89 and 7/21/82 letter

①

①

8/89 letter

The second area involves the declassification instruction. Section 1.5(a)(4) of the Order requires that only a specific date or event, or the notation "Originating Agency Determination Required" (OADR), shall be entered on the "Declassify on" line. Although, your instruction is essentially the same, this modification reflects the Order's requirements. *

If you have any questions concerning this letter, please call Thomas R. Martin, ISOO's liaison to the USTR, on 535-7256, or me on 535-7251.

Sincerely,


Steven Garfinkel
Director

The Honorable
Carla A. Hills
United States Trade Representative
Executive Office of the President
600 17th Street, NW
Washington, DC 20506

✓ cc: Mr. William E. Stuchberry

Sample Page Only
CONFIDENTIAL

This Report Contains Confidential Business Information

**UNITED STATES-ISRAEL FREE
TRADE AGREEMENT: PROBABLE
EFFECTS ON U.S. INDUSTRY
AND CONSUMERS OF
CERTAIN REMAINING U.S.
AND ISRAEL TARIFF
REDUCTIONS**

Report to the President on
Investigation No. 332-265

Volume IV

Export Digests
Nos. 61-87



CLASSIFIED BY: United States Trade
Representative, Letter
Dated February 16, 1989

DECLASSIFY ON: Originating Agency
Determination Required

← *New language*

MARCH 1989

United States International Trade Commission
Washington, DC 20436

CONFIDENTIAL
Sample Page Only



 UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

September 20, 1990

TO: Acting Chairman Brundsale

FROM: Director, Office of Administration

SUBJECT: Approval of Administration's Comments of the Inspector General's Draft Audit Report: "Review USITC's Information Security Program"

On August 14, 1990, the Inspector General submitted copies of the subject audit to each Commissioner by memorandum (IG-N-089). The IG also requested Administration to review the draft audit report and make comments if necessary. In accordance with Section 11 of USITC Directive #1701, "Audit Policies and Procedures", the Office of Administration has sent its comments in draft to the Commissioners, other than you as Chairman, for review. There were no comments submitted by the deadline of September 18, 1990. Confirmation with the staff assistants of Commissioner Rohr, Newquist, and Lodwick was made.

This audit contains a number of findings which are not considered material, but where policies and procedures need to be refined and compliance increased in order to fully comply with the provisions of Executive Order 12356 and the Information Security Oversight Office's regulations.

In accordance with Section 11 of USITC Directive #1701, submitted herewith are Administration's comments for your approval before they are sent to the Inspector General and a copy of the draft audit report. Since the IG has set a deadline of October 1, 1990, for receiving a final response, it would be appreciated if you could indicate your approval, or modification, by the close of business Friday, September 28, 1990.

Approved: ✓

Modify as follows: _____

 Acting Chairman

 9/26/90
 Date

Attachments



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

September 11, 1990

MEMORANDUM

TO: Commissioner Lodwick
Commissioner Rohr
Commissioner Newquist

FROM: Director, Office of Administration

A handwritten signature in cursive script that reads "Tom L. Goodrich".

SUBJECT: Review of Administration's comments on the draft
Inspector General report: "Review of USITC's Information
Security Program"

On August 14, 1990, the Inspector General submitted copies of the subject audit to each of you by memorandum (IG-N-089). In accordance with Section 11 of the USITC Directive 1701, Audit Policies and Procedures, the Office of Administration's response has to be approved by the Chairman and sent to the Inspector General by September 17, 1990. However, procedures contained in USITC Directive 1701 (Section 11.e) provides you the opportunity to comment prior to my sending Administration's comments to the Chairman. Our review of the report is attached. I would appreciate receiving any comments you may have by COB September 18, 1990, so I can send my review to the Chairman by September 20.

This audit contains a number of findings which are not considered material, but where policies and procedures need to be refined and compliance increased in order to fully comply with the provisions of Executive Order 12356 and the Information Security Oversight Office's regulations.

Attachments

cc: Secretary
General Counsel
Director, Office of Investigations
Director, Office of Industries

Director, Office of Economics
Director, Office of Executive and International Liaison
Director, Office of Management Services
Director, Office of Information Resources Management

cc: Vern Simpson
Inspector General w/o attachment

