INSPECTOR GENERAL

IG-V-019

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

May 1, 1998

MEMORANDUM

To: Director, Office of Administration

From: Inspector General Janet Altenhofen

Subject: Inspection Report No 02-98, Review of Commission Policies for Marking Controlled Data

We initiated this inspection in February 1998 to review Commission policies for marking controlled data. In general, we found that Commission policies and practices for marking controlled data were inconsistent. While the inconsistency does not threaten protections for national security or confidential business information, a clearer Commission policy will be both beneficial and welcomed by many Commission officials.

This inspection was conducted by Robert Gellman, Privacy and Information Policy Consultant. We reviewed all relevant legislation and regulations as well as internal policy directives and other Commission publications. Except for national security information, the use of administrative markings has received little or no attention from policy makers. We interviewed the head of each Commission office. In addition, we consulted with officials from the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), the Information Security Oversight Office, and the Office of Personnel Management.

BACKGROUND

In 1978, the Chairman of the Commodity Futures Trading Commission announced that he was throwing into the Potomac River all the rubber stamps used by his agency. He said that this was the only effective way to eliminate confidential stamps. The same year at a congressional hearing on administrative markings, the Chairman of the Subcommittee suggested that there may be quieter ways to achieve a balance between privacy and confidential needs and the requirements

of public availability of government documents.[1] This report was prepared in pursuit of those quieter ways.

The general term used herein to describe the wording placed on documents is *administrative marking*. An *administrative marking* is a mark, sign, stamp, or similar designation consisting of one or more words that characterizes the nature of information in a document. Examples include the markings that identify information classified in the interest of national defense or foreign policy (*confidential*, *secret*, and *top secret*). Other examples are *confidential business information* (CBI), *business proprietary information (BPI)*, *draft*, and *limited official use*. In the past, administrative markings were often applied by rubber stamps. Today, they might just as easily be included in a word processing macro or template.

Except for national security markings, most administrative markings have no legal significance or effect. No matter how an agency record is marked, it may still be the subject of a request under the Freedom of Information Act (FOIA). Information submitted to the Commission marked as CBI or BPI must be protected in accordance with Commission policies, but the information may still be requested and disclosed under the FOIA. Whether any record must be disclosed or can be withheld is determined under FOIA standards, and not by an administrative marking.

In discussing categories of non-public information, it can be difficult to use familiar words with precision. This difficulty is both important for clarity and symptomatic of the challenge of rationalizing the use of administrative markings. Finding a convenient general term for information with disclosure or use restrictions is not easy. Most common terms, such as *secret*, *private*, *restricted*, or *sensitive*, have technical, disclosure-related meanings in some contexts.

Nevertheless, it is necessary to refer generically to the class of data that is, or is believed to be, restricted in use or disclosure. For purposes of this report, this information will be called *controlled information*. This term is used here solely for discussion purposes and is not offered as a new marking.

The true significance of an administrative marking is not always clear from the face of a document. Even the most highly regulated national security markings may not be accurate or properly applied. A document marked *Top Secret* is only properly classified, for example, when the designation was made by an official who has original or derivative top secret classification authority. Other requirements must also be met. Nevertheless, those who see a document marked *top secret* are likely to assume that it has been properly classified and to treat it accordingly. For actual or potential national security information, this conservative assumption is appropriate.

For other information, a stray, casually-applied, or out-of-date marking may take on a life of its own. Information that is not *controlled information* or that no longer qualifies may still be treated

---

[1] *Information Policy Issues Relating to Contractor Data and Administrative Markings*, Hearing before a Subcommittee of the House Committee on Government Operations, 95th Congress (1978).

in the way that it is marked. Unmarked *controlled information* may receive insufficient protection. In either case, the result may be confusion, unnecessary or inadequate security, breaches of important public or private interests, improper treatment for record management and archival purposes, and inconsistent administrative practices. If markings are not reliably and accurately applied, they will lose their cachet and effect. The result can be that administrative markings fade into the background and effectively disappear.

In the 1971 Pentagon Papers case, Mr. Justice Stewart observed that secrecy can be preserved only when credibility is truly maintained. He also warned that:

> When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion.[2]

It is not possible, desirable, or necessary to mark every agency document that may contain *controlled information*. Markings are required throughout government for national security information, and Commission policies result in the marking of investigative documents containing *controlled information*. However, a universal marking policy for all agency documents is not common anywhere in government. The purpose of an administrative marking policy and practice should be to further the objectives of the Commission, and afford appropriate and practical treatment of *controlled information*.

LEGISLATIVE AND REGULATORY BACKGROUND

Statutes and regulations governing the Commission recognize many different categories of *controlled information*. In addition, government-wide policies applicable to or followed by the Commission identify other categories. This discussion of *controlled information* is not comprehensive, but it includes all major categories of interest to Commission operations. The list in Table 1 illustrates the variety of *controlled information*. References are to laws in the U.S. Code (USC), the Code of Federal Regulations (CFR), an Executive Order (EO), or Commission Directives. Some terms are used in more than one source.

The remainder of the report is organized by category of information or marking under four broad groups: Government-wide *Controlled Information*, *Controlled Information* Submitted to the Commission, Personnel, and Internal Commission Markings. Some categories of information could have been placed in more than one group. Each type of information or administrative marking is described along with a discussion of how that information or marking is used at the Commission.

---

[2] *New York Times Co. v. United States*, 403 U.S. 713, 729 (1971) (concurring opinion).

TABLE 1

Terms and Categories Used For Information and Administrative Markings

National Security Information: confidential, *secret*, or *top secret* - EO 12958

Classified Information - 19 USC §1677f(c)(1)(A)

Confidential Business Information - 19 USC §1332(g), 19 CFR §201.6, 19 CFR §201.19,

Business Proprietary Information - 19 USC §1673e(c)(4)(A), 19 CFR §207.7

Proprietary Information - 19 USC §1677f(b)

Privileged Information - 19 USC §1677f(c)(1)(A), 19 CFR §201.6

Confidential Commercial Information - EO 12600

Confidential Information - 19 USC §1337(n), 19 CFR §207.105(b)

Specific Information of a Type for Which There is a Clear and Compelling Need to Withhold From Disclosure - 19 USC §1677f(c)(1)(A)

Customer Names - 19 USC §1677f(c)(1)(A)

Nonnumerical Characterizations of Numerical CBI - 19 CFR §201.6

Nondisclosable Confidential Business Information - 19 CFR §201.6

Information Relating to Allegations Concerning the Commitment of a Prohibited Act - 19 CFR §207.105(b)

Confidential Financial Information - 19 CFR §212.11

Limited Official Use - Directive 1345 (Information Security)

Sensitive Information - Directive 1345 (Information Security)

Report Submitted in Confidence - Directive 1355 (CBI)

Extremely Sensitive CBI - Directive 1355 (CBI)

A. Government-Wide *Controlled Information*

1. National Security Information

Marking documents containing national security information is required under the Executive Order on Security Classification (EO 12958). In addition to the classification level (*confidential*, *secret*, or *top secret*), other information that must be included is the identity of the classifier, the agency of origin, declassification instructions, and reasons for classification. The *portion marking* policy requires that unclassified parts of a document be identified. The Commission follows mandatory government-wide practices for national security information.[3] The marking rules are not subject to alteration by the Commission.

The term *confidential* is of most importance to Commission operations. Under EO 12958, the term has an express, government-wide use meaning for low level national security information. In a more general sense, however, *confidential information* includes any information that may not be publicly disclosed, shared with other agencies, or even circulated within an agency. To the greatest extent possible, *confidential* (as a single word) will only be used here only in the national security context.

The term *confidential* is used routinely at the Commission in a non-national security sense in the phrase *confidential business information*. This phrase is familiar and unavoidable for Commission activities. *Confidential* has no national security connotation when used in this phrase.

Interviews with Commission officials revealed a high degree of awareness of the need to identify and protect national security information. There is evidence of occasional confusion about the use and meaning of the term *confidential* because of its application to both national security information and CBI. One official said that if a document is marked *confidential*, other references are required to determine what kind of information it contains. Another official noted that staff needed more training to learn the distinction between *confidential information* and CBI. Another said that the difference required lots of explanation. Another individual commented on the "unfortunate terminological confusion." However, even where some uncertainty existed, there was no doubt about the need to protect any information marked *confidential*. The ambiguity in the use of *confidential* is discussed below.

---

[3] A recent Inspector General report identified a problem with the original classification procedures for Section 332 reports. This problem has been addressed and resolved. See *Evaluation of 332 Investigations* (Report no. IG-01-98) (Feb. 1998).

The Commission's directive on National Security Information[4] is out of date. EO12356 was replaced in April 1995 by EO 12958 on Classified National Security Information. We understand that efforts are underway to revise Commission directives.[5]

2. Privacy Act

The Privacy Act of 1974[6] defines most personally identifiable information maintained by agencies as *controlled information*. Yet Privacy Act data may still be circulated within an agency, shared with other agencies, or even publicly disclosed at times. Simply designating a document as containing Privacy Act information provides little direction about how it can be used or disclosed. The law does not require marking of Privacy Act information nor is marking recommended by OMB.

A principal source of Privacy Act information at the Commission is personnel files. The Office of Personnel uses a standard, government-wide label on personnel files (Standard Form 66B). The marking *Privacy Act Information* is rarely used at the Commission.

3. Freedom of Information Act

Under the FOIA,[7] nine categories of information may be withheld from public requesters. The FOIA does not require that an agency categorize or mark information at the time of its creation or collection. Most agencies do not decide in advance whether a record contains information that may be exempt from disclosure. Disclosure determinations are normally made only after receipt of a request. This makes sense because much information is never requested and because the disclosability of information changes over time. A document that is exempt today may have to be disclosed tomorrow because of the passage of time or changed circumstances.

For *confidential commercial information* submitted to the government, EO12600[8] calls for a different policy. Each agency must allow a submitter of confidential commercial information to designate, at the time of submission, any information the disclosure of which the submitter claims

---

[4] USITC Directive 1350.1 (2/20/92).

[5] Section 15.c. of ITC Directive 1350.1advises employees that they are subject to criminal penalties in 18 USC §1905, the "Penalty for Disclosing Classified Information". In fact, 18 USC §1905 is titled *Disclosure of Confidential Information Generally*. It applies to the disclosure of trade secrets, and it is one of the statutes that an employee might violate when improperly disclosing CBI or BPI. Other laws criminalize the improper disclosure of national security information. When the directive is revised, the statutory reference should be corrected. Section 4.c. of ITC Directive 1345 on Information Security also mislabels 18 U.S.C. 1905.

[6] 5 USC §552a.

[7] 5 USC §552.

[8] June 23, 1987, 52 Fed. Reg. 23781 (1987).

could reasonably be expected to cause substantial competitive harm. If this marked information is requested under the FOIA, the agency must usually provide predisclosure notice of the request to the submitter. A submitter then has a reasonable period to object to any disclosure.

The Commission's FOIA rules partially implement the policy reflected in EO 12600. For the moment, EO 12600 is most notable for contributing the term *confidential commercial information*, a term not in use at the Commission.

The Commission's FOIA regulations[9] provide for predisclosure notice to submitters of CBI. The regulations differ from EO 12600 in language (*confidential commercial information* for the EO and CBI for the Commission's regulation). They also differ substantively. Under the EO, a submitter of appropriately labelled information is normally entitled to notice before disclosure. A submitter's marking is determinative of the right to notice. Under the Commission's regulations, a submitter receives predisclosure notice only when submitted information *designated by the Commission* as CBI becomes the subject of a request. The Commission's procedures call for a submitter's marking to be accepted or rejected by the Commission at the time of submission. The Commission then gives predisclosure notice only for information accepted and designated by the Commission as CBI.

Because of Commission practices for CBI, the differences between the Commission's FOIA regulations and the requirements of EO 12600 are less significant than they might appear. The Commission's procedure for submitted CBI effectively takes the policy of EO 12600 a step further. Because the sharing of some *controlled information* with parties is common feature of Commission proceedings, an advance determination of confidentiality is essential so that all parties allowed to see the information understand its status. This policy is unusual but clearly justified. Other agencies rarely disclose business-originated *controlled information* outside the agency.

However, some gaps -- mostly theoretical -- remain between the confidentiality procedures for CBI and the FOIA regulations. First, not all submitted *controlled information* becomes part of trade investigations. Some business *controlled information* may come through contracting or other activities. The Commission's FOIA predisclosure notice rules apply only to CBI designated under §201.6 of the Commission's regulations. Contractor data does not appear to qualify.

It is common for federal contractors submitting proposals with potentially proprietary information to mark their information in order to obtain predisclosure notice under agency FOIA rules. A contractor doing business with other agencies might expect to find a marking and notice procedure for submissions to the Commission. A contractor who follows this practice at the Commission, however, will not be clearly entitled to the same notice.

---

[9] 19 CFR §201.19. The Commission's FOIA regulations have not yet been updated to reflect the Electronic Freedom of Information Act Amendments of 1996, Public Law No. 104-231, Act of October 2, 1996. Changes made by the 1996 amendments are not material here. Revisions to Commission FOIA rules are in process.

There is no reason the Commission's FOIA rules should not follow common agency practice in this area and provide contractors an opportunity for predisclosure notice in the event of a FOIA request. Because of the high degree of Commission concern about the improper disclosure of business information, every reasonable precaution should be undertaken.

Accordingly, we suggest that the FOIA regulations be amended to advise submitters of contracting information or other administrative information that they may mark information considered to be proprietary. The regulations should require the Commission to provide notice before any disclosure in response to a FOIA request. The procedures and exceptions in EO 12600 can be followed.

The Commission should use a different term used to identify submitted proprietary information. In order to avoid the proliferation of *confidential*, the regulations should avoid the EO's *confidential commercial information*. Submitters should be advised to mark documents *notify submitter before disclosing*.

Second, the FOIA regulations incorporate the definition of CBI from §201.6. However, on July 22, 1996, the Commission amended that definition.[10] Before the amendment, there was only one type of CBI. Now there are two. The traditional definition of CBI is now accompanied by a second definition for *nondisclosable confidential business information*. The FOIA regulations do not clearly incorporate the new definition. This is not a likely source of confusion. Nor does the actual protection for *nondisclosable CBI* appear threatened as a result. The anomaly is just an unintended result of the 1996 change. However, when the FOIA regulations are changed to provide for predisclosure notice for contractor or administrative data, *nondisclosable CBI* should be referenced along with CBI. The General Counsel disagrees with this conclusion on the grounds that *nondisclosable CBI* is just a subset of *CBI*. However, the regulation is not entirely clear. We continue to believe that any doubts should be resolved in favor of complete clarity.

4. Government in the Sunshine Act

The Government in the Sunshine Act requires agencies like the Commission to conduct open meetings. Some meetings can be closed, and transcripts may be withheld from disclosure. Transcripts of closed Commission meetings and hearings[11] have pink covers and the marking *in camera*. Open meetings have either blue or yellow covers and the marking *public*. No one reports any confusion or problems because of this system.

---

[10] See 61 Federal Register 37818, 37820-21, 37827-28 (July 22, 1996).

[11] See 19 CFR §201.13(m).

5. Equal Access to Justice Act

A Commission regulation[12] implementing the Equal Access to Justice Act requires those applying for an award of fees and expenses to submit a statement of net worth. The statement is ordinarily a public document. However, an applicant may submit a portion of the application marked as *confidential financial information*. A motion to withhold that submission will be resolved by the presiding officer.

Applications under the Equal Access to Justice Act have been rare. Nevertheless, the term *confidential financial information* is troubling because of the use of the word *confidential* and because of its similarity to other terms. A better and more descriptive term might be *Non-public Equal Access to Justice Filing*.

B. *Controlled Information* Submitted to the Commission

The Commission has many statutory and regulatory provisions identifying types of *controlled information*, and different terms are sometimes used to designate the same or similar information. In this section, each type of information and each administrative marking are discussed.

1. CBI and BPI

Many substantive Commission functions involve the submission by a private company of *controlled information*. Commission regulations clearly tell submitters how to mark business data, and no problem with the rules was reported. For some functions (e.g., Title VII investigations), BPI is the term used to describe privately submitted *controlled information*. For other functions (e.g., 337 investigations), the term CBI is used exclusively.[13] Under Commission regulations, both CBI and BPI have the same definition.[14]

Views within the agency about the terms CBI and BPI were mixed. Some officials were not even aware of the use or meaning of BPI. Their offices exclusively used CBI. Some officials knew the difference and relied upon the terms as a signal for identifying the type of investigation to which a document related. Others thought that the use of two terms was unnecessarily confusing and preferred consistent use of BPI. Still others preferred CBI because the word *confidential* conveyed a clear signal about the need to protect the data.

In an ideal world, a single marking for all submitted *controlled information* would be preferable. The use of different terms for marking data with the same meaning is unnecessary. Ideally, the

---

[12] 19 CFR §212.11.

[13] One official pointed out that CBI can also mean *Caribbean Basin Initiative*.

[14] 19 CFR §201.6(a).

term used would not overlap terminologically with any other marking in use. However, the difference in terminology is not a source of sufficient confusion to threaten the Commission's record of protecting *controlled information* it receives from businesses. Everyone interviewed knew the importance of protecting business data, regardless of the mark used.

In addition, changing the terminology would require the cooperation of Commission staff, revision of regulations, amendments to the law, and support from the bar that practices before the Commission. The effort needed to effect a change in information marking for business data would exceed the benefit. Some officials worried that an attempt to change the terminology might be misconstrued by practicing lawyers as a lessening of the Commission's commitment to protecting business data.

In the end, while a good case can be offered for using BPI as the universal marking for business *controlled information*, the case is not sufficiently strong to warrant moving forward. Some intermediate actions can lessen potential confusion and uncertainty.

First, when future changes in the Commission's legislation are considered, attention should be given to the consistent use of terms.[15] Words casually selected by legislative drafters can have consequences in the conduct of Commission business. The Congress should be encouraged to use familiar terms in a manner consistent with current Commission practice.

Second, the differences in usage for BPI and CBI are not readily apparent, even to some veteran Commission staff. We suggest that a description of the practice should be provided in appropriate Commission directives, regulations, and other public documents.

Unless the word *confidential* can be eliminated from use in a business context, the potential always exists for there to be confusion between national security information and CBI. Although we do not recommend eliminating the term CBI, other methods may minimize confusion.

We suggest that the word *confidential* as an administrative marking not be used at the Commission except for CBI and national security information. Rubber stamps with the single word *Confidential* should be discarded.

CBI should continue to be marked *Confidential Business Information*. When national security information is marked by Commission staff, we suggest that the marking *CONFIDENTIAL*

---

[15] The laws regulating Commission activities use a variety of terms to describe *controlled information*. The statutes are not precisely drafted, and inconsistencies can be found. 19 USC §1337(n) refers to *confidential information*. Commission regulations generally call this data *confidential business information*. 19 USC §1673e(4)(A) refers to *business proprietary information*. 19 USC §1677f(b) refers to both *proprietary information* and *business proprietary information*. No apparent distinction between these terms is discernable from the statute.

Classified National Security Information should be used.[16] Classified information received from other agencies is likely to be marked only as *confidential*, but other agencies' practices are beyond the control of the Commission. If appropriate, incoming documents can be remarked as *CONFIDENTIAL Classified National Security Information*.

The general use of the word *confidential* or *confidentiality* should be discouraged because of the lack of clear meaning. A more descriptive phrase is *non-public*. As publications and regulations are revised in the routine course of events, the use of *confidential* can be discontinued.

2. Nondisclosable CBI

The Tariff Act of 1930, as amended,[17] refers to *privileged information, classified information, and specific information of a type for which there is a clear and compelling need to withhold from disclosure*. Commission regulations refer to these three categories generically as *nondisclosable confidential business information*. Some in the agency refer to this information with the informal term *superconfidential*. There is no evidence that documents are marked with that term, however.

Requests from submitters for the designation of *nondisclosable CBI* are rare. The regulations require that *nondisclosable CBI* be marked when submitted using triple brackets.[18] We found no reported problems with the marking of these documents.

3. Customer Names

The Tariff Act of 1930, as amended,[19] also refers to customer names as a separate category of proprietary information with a distinct set of disclosure rules. When Commission staff obtains customer names, the names are treated and marked as BPI. No problems with current practice were reported.

---

[16] The Director of the Information Security Oversight Office raised no objection to the use of this term in place of the single word *confidential*.

[17] 19 USC §1677f(c)(1)(A).

[18] 19 CFR §201.6(b)(3)(C).

[19] 19 USC §1677f(c)(1)(A).

4. Nonnumerical Characterizations of Numerical CBI

Commission regulations defining CBI identify *nonnumerical characterizations of numerical CBI* (e.g., discussions of trends) as a subcategory of CBI. The regulations imply that it will be harder to obtain confidential treatment for this subcategory.[20] We found little evidence that this type of *controlled information* is separately marked or the source of confusion.

5. Declassified CBI/BPI

Section 210.20 of the Commission regulations refers to the *declassification* of confidential information. *Declassification* is a term used in the EO on Security Classification to mean "the authorized change in the status of information from classified information to unclassified information." Its use in the context of CBI has mild potential to be confusing. A better term might be *Redesignated As Public*.

The need to redesignate business data has arisen only occasionally in the past. The new sunset requirements for Commission orders may increase the review of older documents and the need to reconsider the public status of CBI/BPI.

The Commission has defined no procedure or marking policy for former CBI/BPI. The lack of rules has not resulted in any problems, but it may in the future if older documents are more commonly reviewed and redesignated as public. Accordingly, we suggest that a marking policy be established to identify documents that were formerly CBI/BPI. A standard marking should be applied to documents, along with the date of redesignation and the initials of the person who made the decision. It may also be advisable to establish a policy about who is authorized to redesignate CBI/BPI.

6. Information Relating to Allegations About the Commitment of a Prohibited Act

Commission regulations[21] for antidumping investigations define the terms *privileged information* and *proprietary information*. These references break no new ground, although more consistent use of BPI rather than simply *proprietary information* is advisable.

Section 207.105(b) refers to a new subcategory of *controlled information*: *information relating to allegations concerning the commitment of a prohibited act*. The regulation contains no special marking requirement. This type of information is rare.

---

[20] Whether this is really the case is not clear. The standard for the subcategory is *request of the submitter* and *good cause shown*. A request for confidential treatment is required for CBI of any type. Also, a requester must presumably show good cause for all CBI. Thus, whether the standard is actually more stringent is not immediately apparent from the regulation.

[21] 19 CFR §207.3.

7. Administrative Protective Orders

Administrative Protective Orders (APO) are used routinely in some proceedings. The Office of the Secretary's published guide to APOs describes the applicable procedures.[22] The APO process uses the definitions and procedures found in Commission regulations to accomplish its purposes. Some documents are marked *Subject to Protective Order*.

The Administrative Law Judges and other Commission staff universally said that the APO process is well-understood, creates no problems, and accomplishes its purposes. One individual described APOs as "working remarkably well."

8. Extremely Sensitive CBI

The Commission's Directive on Handling and Safeguarding CBI[23] requires "extra precautions" for Commission reports to the President and other reports containing *extremely sensitive CBI*. This is identified as information that "could bring great harm or ruin to a company if disclosed in an unauthorized way." The phrase *extremely sensitive CBI* does not appear elsewhere in Commission rules or directives. No official was familiar with the term or the procedure described for numbering copies and recording responsible individuals. The term is obsolete and should be eliminated when the directive is revised.

9. Report Submitted in Confidence

ITC Directive 1355 also provides rules for the marking of Commission-generated documents containing CBI. The use of *confidential business information* is required on the cover and first page of documents. In addition, all documents must have at the top of each page either *Confidential* or *Report Submitted in Confidence*. Problems with the use of *confidential* have already been discussed. It appears to be more common for the pages of a document to be marked either *Contains Confidential Business Information* or *Contains Business Proprietary Information*.

The phrase *Report Submitted in Confidence* is used by some Commission staff. When the Directive is revised, the phrase might be dropped in favor of something clearer and less ambiguous such as *Non-Public*.

The CBI Directive also describes that portions of a page containing CBI should be marked with brackets or with a double line in the margin. These markings are used without reported problems.

---

[22] U.S. International Trade Commission, An Introduction to Administrative Protective Order Practice in Antidumping and Countervailing Duty Investigations (April 1996) (Office of the Secretary) (Publication No. 2961). The publication is out of date as a result of the July 22, 1996, amendments to Commission regulations. Footnote 4 warns readers of impending changes.

[23] USITC Directive No. 1355, §10.c.(2) (July 1, 1985).

C. Personnel

1. Statements of Employment and Financial Interests

A Commission regulation[24] provides that each statement of employment and financial interests submitted by an employee shall be held in confidence. The regulation does not require that the statement bear any particular administrative marking, and there is no reason to require a marking. The sensitivity of the statements is well understood.

When the Ethics Officer provides written advice to Commission employees, the advice is labelled *Ethics - Confidential.* The word *confidential* should be replaced with a more precise term describing any restrictions on the use or disclosure of the advice. One possibility is to mark the document as *Ethics Advice* and to include a description of any disclosure or use restrictions in the document itself. The General Counsel suggested use of a marking that indicates the document's nonpublic nature, such as "Access Restricted". We concur that a marking would be appropriate, although we note that the phrase "Access Restricted" is not itself clearly descriptive.

2. Postemployment Conflict of Interest

The Commission has a procedure for addressing postemployment conflicts of interest, either through the granting of exceptions or administrative disciplinary hearings. The Chairman has an obligation to take "all necessary steps to protect the privacy of former employees" prior to initiating a disciplinary hearing. Activities under this general authority are rare.

D. Internal Commission Markings

1. Sensitive Information

Section 2.c. of the Commission's Information Security Directive[25] defines the category of *sensitive information.* This term comes from the Computer Security Act of 1987. We found few reported uses of the marking *sensitive information.*

---

[24] 19 CFR §200.735-121.

[25] USITC Directive 1345 (7/31/90).

2. Limited Official Use

A note following section 2.a. of the Information Security Directive refers to the marking *Limited Official Use* (LOU). The note states that information so marked shall be physically handled and transmitted as if it were national security information with the classification *Confidential*. Commission officials reported seeing *LOU* mostly on documents created by other agencies. The marking has been replaced in some cases by *sensitive but unclassified*. Another marking occasionally seen is *for official use only*. There is considerable uncertainty about the meaning and significance of these terms.

3. Eyes Only/To be Opened by Addressee Only

These marking appear routinely on internal Commission documents and envelopes. Commission officials reported a good deal of uncertainty about the precise meaning of the markings. It does not appear that senior staff take the markings seriously. They exercise their own judgment about sharing an *eyes only* document with other staff. The marking is reported to be used mostly on documents containing budget, salary, personnel, and organization information.

4. Privileged

Most Commission officials knew that documents from the General Counsel's office were often marked *privileged*. One other office also uses the term on legal advice to the Commission.

The General Counsel said that written advice about the meaning of privilege circulated many years ago. She said that the term applies to a document that is subject to predecisional, attorney-client, and/or attorney work-product privilege.

Most Commission officials said that they do not understand the significance of the term or how a privileged document may be used or shared. One individual said that the term "doesn't mean anything." Others questioned about why so many documents were marked privileged or why trivial documents were marked. Nearly everyone would welcome clear advice about the significance of privilege.

5. Draft

Commission documents are routinely marked *draft*, but the practice varies from office to office and from individual to individual.

6. Other

Other markings are used occasionally, with practices varying from individual to individual and from office to office. For example, one office had rubber stamps available for use that included: *File Copy*, *Unclassified*, *Priority*, *Air Mail*, *Corrected*, *Completed*, and *Urgent*. Examples of other markings reported to be in use in one or more offices are *May Contain CBI*, *Subject to Protective Order*, *Personnel Sensitive*, *APO Information*, *Confidential Attached*, *Public Inspection*, *Personnel - Official*, and *Expedite*.

Also, the marking *Not for Public Inspection* may be used in investigations into breaches of APO obligations. It is used when non-public documents are shared with a party in order to distinguish between the public and non-public versions of a document.

CONCLUSIONS

There is enough confusion and uncertainty about the use of internal administrative markings to warrant the development of a standard policy. Most officials said that they would welcome a formal policy. It is important, however, that a policy be constructive and not overly formalistic. Any policy should seek to accomplish these objectives:

- A policy should define the meaning of markings for internal use so that senders and recipients have the same understanding of what each term means and how a marked document may be used, disclosed, and discarded.

- Internal administrative markings should not be mandatory. Staff should have discretion to decide whether to use a marking, and each office should be allowed to establish a local policy as long as it is consistent with the overall policy. Existing policies for the mandatory marking of national security information, CBI, and BPI should not be changed, however.

- No attempt should be made to define every possible marking. *Draft* is an example of a term that needs no explanation.

- Markings that should be defined include: *privileged*, *eyes only*, *to be opened by addressee only*, and *limited official use*. There may be a need to define new markings with clearer meanings, such as *no external distribution*.

- The policy should make a distinction between markings placed on an envelope and markings placed on a document. An envelope might be marked *to be opened by addressee only*, but the document inside may require a different marking or none at all. If a document is addressed to one individual with copies to others, markings should be applicable to all recipients or not used.

• The policy should encourage authors of documents with complex use or disclosure rules to explain the rules in the document rather than to rely on a marking.

SUGGESTIONS

We suggest that the Director of Administration, in his capacity as Chairman of the Information Security Committee:

1. Amend the FOIA regulations to (a) permit contractors, bidders, and others who have an administrative relationship with the Commission to receive notice before release of their submission under the FOIA by marking the submission; and (b) include an appropriate reference to *nondisclosable CBI*.

2. Issue an administrative announcement that the word *confidential* as an administrative marking should not be used except for CBI and national security information. All rubber stamps with the single word *confidential* should be replaced with a stamp *CONFIDENTIAL Classified National Security Information*. The markings *Confidential Business Information* and *CBI* should continue in use.

3. Explain usage practices for CBI and BPI to Commission staff, and establish a policy to identify and mark documents that have lost their status as CBI/BPI.

4. Revise directives, regulations, and policy documents to ensure that administrative marking terms are used with precision.

5. Establish a policy on the internal use of administrative markings to clarify the meanings of terms and standardize practice.

cc: Commission
Information Security Committee