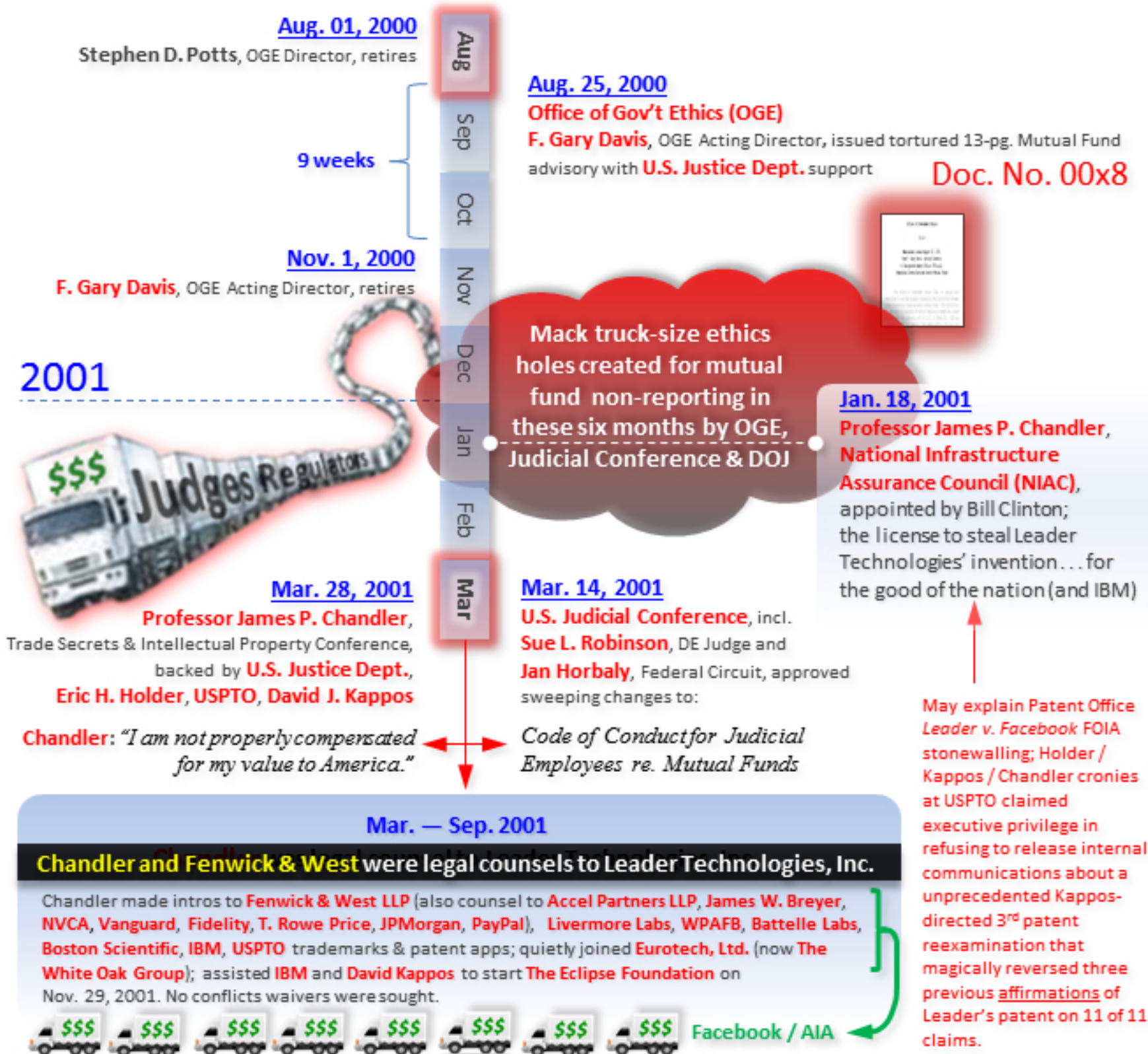


The Scene of the Crime:

THE GREAT MUTUAL FUND SCAM

In 2000-2001, **Office of Gov't Ethics (OGE)**, **Judicial Conference** and **DOJ** officials fabricated a convoy of self-serving advisory opinions for reporting mutual fund holdings



Sources: PACER, GPO, IBM, Eclipse, DOJ, SEC Edgar, OGE, USPTO, Leader, NIPU, Fenwick & West, archive.org, whitehouse.gov, archives.gov, FINRA, sec.gov, Judicial Conference, US Courts. <http://www.oge.gov/OGE-Advisories/Legal-Advisories/00x8-Diversified-and-Sector-Mutual-Funds/> | <http://www.uscourts.gov/FederalCourts/JudicialConference/Proceedings/Proceedings.aspx?doc=/uscourts/FederalCourts/judconf/proceedings/2001-03.pdf> | <http://www.fbcovr.com/docs/chandler/2001-01-18-Members-named-to-National-Infrastructure-Assurance-Council-Bill-Clinton-White-House-Jan-18-2001.pdf>

Office of Government Ethics

00 x 8

**Memorandum Issued August 25, 2000,
from F. Gary Davis, Acting Director,
to Designated Agency Ethics Officials
Regarding Diversified and Sector Mutual Funds**

The Office of Government Ethics (OGE) is issuing this memorandum to provide guidance concerning the distinction between diversified mutual funds and sector mutual funds. This distinction is important for purposes of certain regulatory exemptions issued by OGE under the authority of 18 U.S.C. § 208(b)(2). OGE has received a number of requests from agency ethics officials for advice in this area. Moreover, OGE recently concluded a survey of agency experience and satisfaction with the regulatory exemptions, which are codified in subpart B of 5 C.F.R. part 2640. It was apparent from several of the responses that there was demand for legal and practical guidance concerning the application of the rules pertaining to diversified and sector mutual funds. The advice contained in this memorandum is an effort to meet that demand.

We note at the outset that this memorandum is intended only to provide general guidance. It is impossible not to take notice of the great number and variety of mutual funds on the market today. Moreover, one can easily imagine that new variations will continue to appear in the future, as fund managers respond to new investment opportunities and other developments in the economy. OGE's attempt in this memorandum to list representative types of sector and diversified funds is necessarily tentative and incomplete. Moreover, although OGE has been able to identify some common features of certain types of funds, we also have encountered occasional exceptions where, for example, the name of a fund would not be a conclusive indicator of the fund's investment concentration, for purposes of part 2640. Consequently, employees and ethics officials always will need to consider the characteristics of any given fund, including the nature and scope of any "sector" in which the fund manager may purport to specialize.

We also want to make clear that nothing in this memorandum is intended as an endorsement or disparagement of any particular mutual fund or type of mutual fund. For this reason, the discussion below generally omits specific fund names. Federal employees remain free to invest as they choose, subject to any

prohibited financial interest restrictions, as described in 5 C.F.R. § 2635.403, and any disqualification obligations, as described in 5 C.F.R. part 2640.

EXEMPTIONS UNDER 18 U.S.C. § 208(B) (2)

Section 208(a) of Title 18, United States Code, prohibits an employee from participating in any particular matter in which the employee, or any other person specified in the statute, has a financial interest. The prohibition has been interpreted as applying to financial interests in official matters affecting the underlying holdings of a mutual fund. See, e.g., OGE Informal Advisory Letter 93 x 27. OGE has authority, however, to promulgate regulations exempting certain types of financial interests from this prohibition, where OGE determines that the interest is too remote or inconsequential to affect the integrity of the services of the Government employees to whom the exemption applies. 18 U.S.C. § 208(b) (2). Subpart B of part 2640 contains a number of such exemptions, several of which are applicable to interests in mutual funds.¹ The distinction between diversified and sector mutual funds is particularly important for certain of these exemptions.

A. Exemption for Diversified Mutual Funds

Subpart B contains a relatively broad exemption for any disqualifying financial interest arising from the ownership of a "diversified mutual fund." 5 C.F.R. § 2640.201(a). Provided that the fund meets the definition of "diversified," set out in section 2640.102(a), an employee may participate in any matter affecting any of the underlying holdings of the mutual fund, without regard to the magnitude of the employee's interest in the fund. Such an expansive exemption was deemed justified because, among other reasons, diversified funds hold "securities of issuers who are engaged in a variety of businesses or industries." 60 Fed. Reg. 47207, 47211 (September 11, 1995) (preamble to proposed rule). Under such circumstances, it is likely that any Government action affecting a given issuer would have only a diffuse or negligible effect on the employee's financial interest in the overall fund.

¹ For purposes of part 2640, "mutual fund" is defined as "an entity which is registered as a management company under the Investment Company act of 1940, as amended (15 U.S.C. § 80a-1 et seq.)" 5 C.F.R. § 2640.102(k). This includes open-end, closed-end and exchange-traded mutual funds, and registered money market funds.

The definition of diversified, obviously, is of critical importance. Basically, as OGE stated in the preamble to the final rule, "the exemption for diversified mutual funds applies to *all mutual funds except sector funds*." 61 *Fed. Reg.* 66829, 66833 (December 18, 1996) (emphasis added). Recognizing that sector and diversified might mean different things in different contexts, OGE specifically described the kind of sector/diversified distinction it had in mind: "Diversified means that the fund . . . does not have a stated policy of concentrating its investments in any industry, business, single country other than the United States, or bonds of a single State within the United States" 5 C.F.R. § 2640.102(a).

If a fund does have a stated policy of concentrating its investments in such a sector, OGE determined that the broad exemption of section 2640.201(a) would not apply because of heightened conflict of interest concerns. The possible effect of some particular matters on certain sector funds is much more focused and potentially substantial than would be the case with a diversified fund. Indeed, it is quite common for a sector fund prospectus to include some cautionary statement indicating the greater risk of volatility resulting from concentration in areas affected by Government regulation or spending. A Federal employee could participate in an important rulemaking proceeding that impacts many or all members of a given industry, thus affecting not only a number of the underlying holdings of a relevant sector fund but even the overall economic outlook for the sector in which the fund specializes. Employees whose duties affect companies in a discrete industry, business, etc., can have an appreciable conflict of interest if they invest heavily in mutual funds that specialize in that very sector.

B. Exemptions Applicable to Sector Mutual Funds

Nevertheless, OGE has promulgated certain other exemptions that may apply to interests in sector funds. For those mutual funds that do not meet the diversification standard, three exemptions are especially important.²

² Depending on the circumstances, other exemptions in subpart B may apply to certain interests in sector funds, but the three exemptions discussed here are the most commonly applicable. Note, however, that no regulatory exemption applies to any mutual fund that is a prohibited interest, pursuant to 5 C.F.R. § 2640.204, although many agency-specific prohibitions make some exception for the holding of funds not focused on a sector that is problematic for the particular agency. See, e.g., 5 C.F.R. § 3401.102(c)(1) (Federal Energy Regulatory Commission).

First, section 2640.201(b) expressly applies to certain interests in a sector mutual fund. For purposes of this exemption, sector mutual fund is defined essentially by contrast with the definition of diversified fund: "Sector mutual fund means a mutual fund that concentrates its investments in an industry, business, single country other than the United States, or bonds of a single State within the United States." 5 C.F.R. § 2640.102(q). With respect to such funds, section 2640.201(b) permits an employee to participate in any particular matter where the disqualifying interest arises solely from the "non-sector" holdings of the fund, i.e., those incidental holdings that are outside of the fund's express area of concentration. Thus, for example, an employee who owns a telecommunications sector fund may participate in certain energy matters, notwithstanding the fact that the fund may hold securities of an affected energy company.

Second, because part 2640 currently treats sector funds as "publicly traded securities," interests in such funds are covered by the \$5,000 de minimis exemption for particular matters involving specific parties. 5 C.F.R. §§ 2640.102(p) & (r); 2640.202(a). Thus, for example, an employee owning up to \$5,000 in a financial services sector fund may participate in the investigation of a bank whose stock is held by the fund. The \$5,000 limit would apply to the aggregated value of all affected sector funds held by the employee, the employee's spouse, and the employee's minor children. 5 C.F.R. § 2640.202(a)(2). Moreover, as with all of the de minimis exemptions discussed here, it should be noted that the value limit applies to the value of the person's interest in the fund as a whole, not the pro rata value of any underlying holding of the fund. See 61 *Fed. Reg.* at 66835-36.

Third, by the same token, the current de minimis exemption for particular matters of general applicability covers interests in sector mutual funds. 5 C.F.R. § 2640.202(b). An employee may participate in a matter of general applicability where the disqualifying interest arises from aggregated holdings of up to \$25,000 in any one affected sector fund and \$50,000 in all affected sector funds owned by the employee, the employee's spouse, and the employee's minor children. Thus, for example, an employee who owns \$10,000 in one health sector fund and \$20,000 in another health sector fund may participate in a Medicare policy decision affecting a certain class of healthcare providers, including issuers of securities held by the two funds.

Finally, in connection with the subject of de minimis interests, we note that OGE anticipates proposing a new de minimis exemption in the near future specifically for sector funds. The exemption, if adopted, would create a higher limit of \$50,000 for all particular matters. The \$50,000 de minimis level would apply

to all interests in affected funds focused on the same sector, whether owned by the employee, the employee's spouse, or the employee's minor children. OGE believes that such an exemption would be justified because interests in the underlying holdings of a sector fund are more remote and inconsequential than direct ownership by the employee of securities in an affected issuer. Nevertheless, the basic distinction between diversified and sector funds will remain, since OGE does not intend to propose an unlimited exemption of the type that currently exists for diversified funds.

DISTINGUISHING SECTOR AND DIVERSIFIED FUNDS

As indicated above, the distinction between sector and diversified funds turns on whether the fund has an express policy of "concentrating its investments in *any industry, business, single country other than the United States, or bonds of a single State* within the United States." 5 C.F.R. § 2640.102(a) (emphasis added). This standard differs somewhat from other rules that establish the requisite degree of diversification for different purposes, and any guidance herein should not be confused with guidance pertaining to those other standards of diversification. Compare 5 C.F.R. § 2634.1003(c)(1) (permitted rollover property for certificates of divestiture); § 2634.310(c)(3) (excepted investment funds); § 2634.404(b)(2) (diversified trusts). Unlike some of these other standards, the focus of part 2640 is not whether a fund concentrates on a broadly defined "economic," "geographic" or "regional" sector, but rather a somewhat narrower "industry," "business," "single country" or "bonds of a single State."

A. Industry or Business Sector

Agencies occasionally have questions about whether a particular fund really concentrates on an "industry" or "business," as opposed to a broader economic sector that includes a significant variety of independent industries or businesses. Determining what is an industry or business sector, therefore, is crucial for purposes of the relevant exemptions. Moreover, such determinations necessarily involve the exercise of some judgment, taking into account the stated policies of the fund and any common features of the companies in which it specializes.

OGE is aware of no universally accepted criterion for what constitutes an "industry" or "business" that would be useful for this purpose. Any conceivable classification of the economy by industry groupings would involve numerous judgments about what degree of similarity in operations or interests among firms would be sufficient to place them within a single industry. One can distinguish among companies on so many different levels, and with

such varying degrees of detail, that it is possible to describe a virtually infinite number of classes and subclasses. For example, the North American Industry Classification (NAIC) system, used by the United States for a variety of statistical and other purposes, now divides the economy into twenty broad "sectors," whereas the Standard Industrial Classification (SIC) system, which was used until recently, had only ten sectors. Even under NAIC, some sectors are defined very broadly (e.g., "Manufacturing," which includes a great diversity of manufacturing operations), whereas other sectors are seemingly more narrow (e.g., "Health Care and Social Assistance"). Moreover, under both systems, there are several levels of subdivision within each sector, thus indicating the possibility of ever more refined distinctions among industries and sub-industries³. More important, some ways of grouping industries and businesses, while relevant for certain statistical and other purposes, may be wholly inadequate for conflict of interest purposes. For example, according to NAIC, medical equipment and pharmaceuticals are not only separate "industries," but also they are in different "industry groups" and even different manufacturing "sub-sectors" altogether; from a Federal conflict of interest perspective, however, drugs and medical devices are not only regulated by the same agency (the Department of Health and Human Services) and subject to many related regulatory requirements, but also it has been recognized that certain medical devices and drugs may be complementary or even competing products for the same medical condition.

Therefore, in addressing the question of what constitutes an industry or business, for purposes of identifying a sector fund, OGE has attempted to take a pragmatic approach. In doing so, OGE has taken into account both the need for clarity and the need for criteria that are relevant to the purposes of the executive branch ethics program. In some respects, the best guidance in this area would be examples of decisions OGE has already made in applying the standard, rather than abstract statements of general principle. Nevertheless, before setting out a list of examples of representative types of sector and diversified funds (see below), we believe there is at least some utility in articulating the general approach that governs OGE's application of the diversification standard.

³ NAIC uses six-digit codes breaking the economy down according to sector, subsector, industry group, industry, and U.S. industry. SIC used a four-digit system indicating division, major group, industry group, and industry code.

B. Basic Approach

Basically, OGE approaches such questions by examining the degree of relatedness and overlapping interests and operations among the types of companies in which a given mutual fund specializes. As suggested above, this inquiry also is performed in the context of realistic conflict of interest considerations, as well as the need for some measure of common sense. Given the latter considerations, OGE will deem certain arguably discrete types of companies to be part of one industry or business sector if, for example, they share a common regulatory environment or if Government decisions affecting one type of company would be expected to affect the other, given their interdependence or competition with each other.

This approach is embodied in part 2640 itself. In example 2 following section 2640.202(b), OGE indicates that a particular fund is not diversified because "it is invested in health-related companies such as pharmaceuticals, developers of medical instruments and devices, managed care health organizations, and acute care hospitals." See also 61 Fed. Reg. at 66833 (preamble to final rule cites "Vanguard Specialized Portfolios: Healthcare" as example of sector fund). OGE acknowledges that, for certain economic and other purposes, one could argue that this fund does not describe a single sector but rather a cluster of discrete types of businesses, each occupying an identifiable niche within the multifaceted sphere of health care and health science. Primarily for conflict of interest reasons, however, OGE has chosen to focus rather on the common denominator of health to describe the relevant sector. Despite their differences, the types of companies in which this fund specializes are significantly interdependent, and Government decisions affecting one type often will affect the others. For example, Government decisions concerning the reimbursement of health care providers (e.g., hospitals) for certain services can have an impact on the manufacturers of the medical products (e.g., drugs and medical devices) specifically used in connection with those services.

In a similar vein, example 2 following section 2640.201(a) indicates that a fund "that expressly concentrates its holdings in the stock of utilities companies" is not diversified. OGE is aware that utility funds may define their concentration as including companies involved in such areas as electricity, gas, water, sanitation systems, telecommunications (mainly telephone service), and cable television. As diverse as these areas may be for some purposes, OGE generally believes that utility funds are properly treated as sector funds. Many of these types of utility companies have common interests in the use of rights of way for transmission and distribution, are sensitive to energy prices, and may even

compete with each other in some respects. Moreover, according to one prospectus OGE reviewed, "telephone and electric companies dominate the utility stock market," thus indicating a further degree of potential concentration within the sector. (See the discussions below concerning "dual industry" funds and "real focus" vs. miscellaneous sectors.) OGE also recognizes the practical need to draw a line that can be easily understood and applied in various situations; utility funds are fairly common, and OGE believes that historically they have been regarded as sector funds within the ethics community.

We want to emphasize, however, that a fund will not be deemed a sector fund where the manager describes essentially generic categories of concentration. Relatively general or superficial similarities among a group of disparate industries or businesses will not be sufficient to trigger the stricter treatment OGE has reserved for sector funds. Several examples would be "entertainment," "leisure," "consumer products," "cyclicals," and "venture capital" funds. Another common example would be generic "science" or "technology" funds. Most of the science and technology funds we have reviewed do not focus on any particular scientific or technological industry, but rather a variety of industries, including biotechnology, computers, telecommunications, environmental services, aerospace, etc., which have little in common except a commitment of resources to research and development in scientific fields.⁴

In some cases, of course, the distinction between a sector and a diversified fund can be difficult to draw because the distinctions among certain industries may be blurred. The case of "financial services funds" illustrates this problem. On the one hand, there is little question that "banking funds" should be treated as sector rather than diversified funds; prospectuses for such funds often indicate a fairly specific focus, such as companies engaged in accepting deposits and making commercial and principally non-mortgage consumer loans, including state chartered banks, savings and loan institutions, and banks that are members of the Federal Reserve System. On the other hand, the question is somewhat closer with respect to the broader category of financial services funds. Some of the prospectuses for these funds define the financial services sector as including, in addition to the

⁴ We should caution, however, that we have reviewed the prospectus for at least one self-described "technology" fund that expressly focused on computers and electronics, and another prospectus for a "high technology" fund that expressly focused on computer and related companies; we believe such funds are not diversified, despite their names.

types of banks described above, such companies as: "brokerage and advisory firms;" "leasing companies;" "insurance firms;" "publicly traded, government-sponsored financial enterprises;" "home, auto, and other specialty finance companies;" "electronic trading networks;" "electronic transaction processors for financial services companies;" and "diversified financial companies." Nevertheless, OGE has determined that financial services funds generally should be viewed as sector funds. See 60 *Fed. Reg.* at 47213. As one fund prospectus notes, "the financial services industries . . . can be subject to relatively rapid change due to increasingly blurred distinctions between service segments," and all can be "significantly affected by availability and cost of capital funds, changes in interest rates, and price competition." OGE believes that there is enough potential for competition among the types of companies within the sector, as well as potential for certain particular matters to affect more than one type, that funds focused on financial services companies should not be treated as being diversified, for purposes of part 2640.

Along the same lines, OGE generally considers "dual industry" funds to be nondiversified. These funds are expressly marketed as being concentrated in two industry or business sectors, such as "defense and aerospace," "telecommunications and utilities," or "media and telecommunications." OGE usually treats such dual industry funds as being sector funds, under part 2640, for essentially two reasons. First, rarely would two unrelated industries be yoked together arbitrarily. Usually, one would assume that the fund manager perceives that the two sectors are related in some significant way. Indeed, in many instances, one could argue that the prospectus really describes only two aspects of a single industrial sector. Second, we believe that a fund that is expressly focused on two sectors is still sufficiently concentrated in each sector to pose the kinds of risks associated with sector funds.

DETERMINING A FUND'S INVESTMENT POLICY

Before providing a list of examples of how OGE has applied this general approach to several types of sector and diversified funds, it is necessary to address one last issue that has generated some confusion. Agency ethics officials commonly ask what it means for a fund to have a "stated policy" of concentrating its investments in a sector. In other words, where and how can one find the concentration policy of a particular fund?

On one level, this involves the very practical question of where to look for such a policy. The rule notes that whether a mutual fund meets the diversification standard "may be determined by checking the fund's prospectus or by calling a broker or the

manager of the fund." 5 C.F.R. § 2640.102(a) (Note). Many fund prospectuses are readily available to employees and ethics officials through various means, including the Internet. Typically, such prospectuses have statements indicating the "principal investment strategy," "fund objective," or other provisions that make reference to any sector concentration policy. Moreover, as we have advised in the past, "[o]ften, it is possible to learn whether a fund is a sector fund simply from the fund's name (i.e., Vanguard Specialized Portfolios: Healthcare)." 61 Fed. Reg. at 66833. OGE also has found that other convenient resources, such as publications and certain online mutual fund guides, can provide quick and understandable descriptions of many fund concentration policies, although such aids may not be as current or reliable as the fund prospectus in some instances.

We must emphasize that OGE's focus is on the *stated* policy of the fund manager, not on the actual breakdown of fund holdings at any given point in time.⁵ The actual portfolio of investments in a particular fund is subject to change, including the relative concentrations in certain sectors. Therefore, OGE has determined that a more reliable and consistent measure of concentration, for purposes of the exemptions in part 2640 anyway, is the fund's express statement of overall concentration philosophy. The relevant starting point, therefore, is not a printout of a fund's recent holdings or even a list of the fund's top five or ten holdings, but rather the fund's statement of basic concentration policy.

OGE is aware that ethics officials sometimes may note an apparent "disconnect" between the level of diversification espoused in a fund's policy statement and the level of concentration reflected in the fund's actual holdings at a given time. For example, OGE recently reviewed the prospectus of a particular "science and technology fund," whose statement of concentration policy described a significant diversity of businesses and industries: "electronics; communications; e-commerce; information services; media; life sciences and health care; chemicals and synthetic materials; and defense and aerospace." At the same time, the fund's top ten holdings seemed disproportionately weighted in computer and computer-related industries. The ethics official who brought this to our attention asked whether computer procurement specialists at her agency could own such a fund without risking

⁵ This approach differs, for example, from the financial disclosure rule applicable to excepted investment funds, which defines "widely diversified" according to the actual portfolio composition at a specific time in the reporting period. See 5 C.F.R. §2634.310(C)(3).

problems under 18 U.S.C. § 208; we advised that this fund was covered by the exemption for diversified mutual funds. In such cases, the definitions of "diversified" and "sector mutual fund," in part 2640, require that the focus remain on the stated policy in the prospectus, not the actual fund portfolio at any historical point. Not only is this result compelled by the rule, but it is consistent with the reality that relative sector concentrations may change frequently and with little or no notice, within the limits of the stated fund policy.

Occasionally, there also may be issues concerning the central focus of a fund, as described in the prospectus. For example, agencies sometimes may question whether references in a prospectus to "other" or miscellaneous sectors are sufficient to render a fund diversified when it would otherwise appear to be a sector fund. In this connection, OGE recently reviewed the prospectus of a self-described "internet fund" that included a fairly typical description of an Internet sector concentration policy: "companies . . . engaged in the research, design, development or manufacturing, or engaged to a significant extent in the business of distributing products, processes or services for use with Internet or Intranet related businesses." However, the prospectus then went on to state that the fund "may also invest in other 'high tech' companies," which it defined as "firms in the computer, communications, video, electronics, office and factory automation and robotics sectors." OGE determined that the main thrust of the stated concentration policy of this fund remained Internet-related companies, notwithstanding the discretion of the fund manager to "minor" in other areas of technology that are more or less tangential to the core Internet focus. Obviously, such questions are matters of degree, and a fund should be regarded in light of the overarching investment strategy articulated in the prospectus and any other statements from the fund manager. Moreover, as a practical matter, the name by which a fund is marketed (e.g., "ABC Internet Fund") sometimes may help to settle close questions as to the core focus.

EXAMPLES OF SECTOR AND DIVERSIFIED FUNDS

As stated above, the best guidance in this area probably is OGE's experience with specific types of mutual funds. Subject to the caveats expressed earlier, particularly the need to consider any peculiarities of a given fund and its prospectus where appropriate, the following lists provide examples of common types of funds with respect to which OGE generally has been able to discern a policy of sector concentration or diversification. Please note that these lists are not intended to be comprehensive or static.

A. Sector Fund Examples

OGE's general experience has been that mutual funds promoted as having the following areas of concentration are likely to be sector funds:

- Utilities
- Telecommunications
- Energy
- Health Care/Health Sciences
- Life Sciences
- Financial Services
- Banking
- Brokerage & Investment Management
- Precious Metals
- Gold
- Biotechnology
- Food & Agricultural Products
- Media
- Automotive
- Chemicals
- Computers
- Electronics
- Internet
- Japan/Mexico/etc.
- California/Maryland/etc. Bonds
- GNMA
- Real Estate
- REIT
- Defense & Aerospace
- Transportation
- Housing & Construction

Note that some of the above sectors are not mutually exclusive but may overlap to a significant degree or even subsume others, depending on how the fund manager defines the concentration policy. For example, depending on the focus described in the prospectus, a

biotechnology fund might significantly overlap with the health sciences or life sciences sector, or a utilities fund might significantly overlap with either the energy or telecommunications sector. In some cases, therefore, ethics officials and employees still may need to look beyond the fund name to the prospectus, in order to determine whether there is a conflict between the sector fund's actual focus and an employee's expected duties.

B. Diversified Fund Examples

The following types of funds generally have been found by OGE to be diversified for purposes of the exemptions in part 2640:

Leisure/Entertainment
Research
Generic "Science"/"Technology"⁶
Venture Capital
Pacific/European/South Asian/etc.
Generic "Index"/"S&P"/etc.
Generic "Growth"/"Income"/"Capital Appreciation"/"High Yield"/"Value"/etc.
Generic "Equity"/"Bond"
Generic "Municipal"
Generic "Tax-Free"
Emerging Markets
Cyclicals
Small Cap/Mid Cap/Large Cap
Balanced
Consumer Products/Services
Natural Resources
Basic Materials/Industrial Materials
Money Market⁷
U.S. Treasury

⁶ But note the caution at footnote 4 above.

⁷ This includes only money market mutual funds, not bank deposit money market accounts, which are not mutual funds. See 60 Fed. Reg. at 47213.

**REPORT OF THE PROCEEDINGS
OF THE JUDICIAL CONFERENCE
OF THE UNITED STATES**

*MARCH 14, 2001
WASHINGTON, D.C.*

**REPORT OF THE PROCEEDINGS
OF THE JUDICIAL CONFERENCE
OF THE UNITED STATES**

*MARCH 14, 2001
WASHINGTON, D.C.*

*JUDICIAL CONFERENCE OF THE UNITED STATES
CHIEF JUSTICE WILLIAM H. REHNQUIST,
PRESIDING
LEONIDAS RALPH MECHAM, SECRETARY*

REPORT OF THE PROCEEDINGS OF THE JUDICIAL CONFERENCE OF THE UNITED STATES

March 14, 2001

Contents

Call of the Conference	1
Reports	4
Elections	4
Executive Committee	4
Financial Disclosure Legislation	4
Federal Courts Improvement Bill	4
Miscellaneous Actions	5
Committee on the Administrative Office	6
Wiretap Reports	6
Committee Activities	7
Committee on Automation and Technology	7
Long Range Plan for Information Technology	7
Location of Court Records	7
Committee Activities	8
Committee on the Administration of the Bankruptcy System	8
Reappointment of Bankruptcy Judges	8
Place of Holding Bankruptcy Court	9
Committee Activities	9
Committee on the Budget	10
Transfer of Retirement Funds	10
Committee Activities	10
Committee on Codes of Conduct	10
Code of Conduct for Judicial Employees	10
Committee Activities	12
Committee on Court Administration and Case Management	12
Miscellaneous Fee Schedules	12
Civil Litigation Management Manual	15
Juror Qualification Questionnaire	15
Social Security Reporting Requirements	15
Committee Activities	16
Committee on Criminal Law	17
Risk Prediction Index	17

Judgments in a Criminal Case	17
Committee Activities	17
Committee on Defender Services	18
Community Defender Organization Grant and Conditions Agreement ..	18
Reasonable Accommodations for Employees with Disabilities	18
Professional Liability Insurance	19
<i>Amicus Curiae</i> Policy for Federal Defenders	20
Use of CJA Resources	20
Committee Activities	21
Committee on Federal-State Jurisdiction	21
Resident Alien Proviso	21
Committee Activities	22
Committee on Financial Disclosure	22
Committee Activities	22
Committee on Intercircuit Assignments	23
Committee Activities	23
Committee on International Judicial Relations	23
Committee Activities	23
Committee on the Judicial Branch	23
Judicial Compensation	23
Committee Activities	24
Committee on Judicial Resources	24
Biennial Survey of Judgeship Needs	24
Reasonable Accommodation for Employees with Disabilities	25
Professional Liability Insurance	26
Recruitment and Retention Bonuses	26
Law Clerk Student Loans	26
Committee Activities	27
Committee on the Administration of the Magistrate Judges System	27
Reimbursement Regulations	27
Changes in Magistrate Judge Positions	28
Committee Activities	30
Committee to Review Circuit Council Conduct and Disability Orders	31
Committee Activities	31
Committee on Rules of Practice and Procedure	31
Committee Activities	31
Committee on Security and Facilities	32
Construction Submission Process/Five-Year Courthouse Project Plan ..	32
Release of Space	32
Ergonomics in the Judicial Workplace	33
Bankruptcy Jury Boxes	33
Committee Activities	33
Funding	34

**REPORT OF THE PROCEEDINGS
OF THE JUDICIAL CONFERENCE
OF THE UNITED STATES**

March 14, 2001

The Judicial Conference of the United States convened in Washington, D.C., on March 14, 2001, pursuant to the call of the Chief Justice of the United States issued under 28 U.S.C. § 331. The Chief Justice presided, and the following members of the Conference were present:

First Circuit:

Chief Judge Juan R. Torruella
Chief Judge D. Brock Hornby,
District of Maine

Second Circuit:

Chief Judge John M. Walker, Jr.
Judge Charles P. Sifton,
Eastern District of New York

Third Circuit:

Chief Judge Edward R. Becker
Chief Judge Sue L. Robinson,
District of Delaware

Fourth Circuit:

Chief Judge J. Harvie Wilkinson III
Chief Judge Charles H. Haden II,
Southern District of West Virginia

Fifth Circuit:

Chief Judge Carolyn Dineen King
Judge Hayden W. Head, Jr.,
Southern District of Texas

Sixth Circuit:

Chief Judge Boyce F. Martin, Jr.
Judge Thomas A. Wiseman, Jr.,
Middle District of Tennessee

Seventh Circuit:

Chief Judge Joel M. Flaum
Chief Judge Marvin E. Aspen,
Northern District of Illinois

Eighth Circuit:

Chief Judge Roger L. Wollman
Judge James M. Rosenbaum,
District of Minnesota

Ninth Circuit:

Chief Judge Mary M. Schroeder
Judge Judith N. Keep,
Southern District of California

Tenth Circuit:

Chief Judge Deanell R. Tacha
Chief Judge Frank Howell Seay,
Eastern District of Oklahoma

Eleventh Circuit:

Chief Judge R. Lanier Anderson
Chief Judge Charles R. Butler, Jr.,
Southern District of Alabama

District of Columbia Circuit:

Chief Judge Harry T. Edwards
Judge Thomas F. Hogan,¹
District of Columbia

Federal Circuit:

Chief Judge Haldane Robert Mayer

Court of International Trade:

Chief Judge Gregory W. Carman

Circuit Judges W. Eugene Davis, David R. Hansen, Dennis G. Jacobs, Jane R. Roth, Anthony J. Scirica, Walter K. Stapleton, and William W. Wilkins, Jr., and District Judges Lourdes G. Baird, Robin J. Cauthron, John G. Heyburn II, David F. Levi, John W. Lungstrum, Edwin L. Nelson and Harvey E. Schlesinger attended the Conference session. Jan Horbaly of the Federal Circuit represented the Circuit Executives.

Leonidas Ralph Mecham, Director of the Administrative Office of the United States Courts, attended the session of the Conference, as did Clarence A. Lee, Jr., Associate Director for Management and Operations; William R. Burchill, Jr., Associate Director and General Counsel; Karen K. Siegel, Assistant Director, Judicial Conference Executive Secretariat; Michael W. Blommer, Assistant Director, Legislative Affairs; David Sellers, Assistant Director, Public Affairs; and Wendy Jennis, Deputy Assistant Director, Judicial Conference Executive Secretariat. Judge Fern Smith and Russell Wheeler, Director and Deputy Director of the Federal Judicial Center, also attended the session of the Conference, as did Sally Rider, Administrative Assistant to the Chief Justice.

Senator Jeff Sessions and Representatives Howard Coble and F. James Sensenbrenner spoke on matters pending in Congress of interest to the Conference. Attorney General John Ashcroft addressed the Conference on matters of mutual interest to the judiciary and the Department of Justice.

¹Designated by the Chief Justice.

REPORTS

Mr. Mecham reported to the Conference on the judicial business of the courts and on matters relating to the Administrative Office (AO). Judge Smith spoke to the Conference about Federal Judicial Center programs, and Judge Diana E. Murphy, Chair of the United States Sentencing Commission, reported on Sentencing Commission activities.

ELECTIONS

The Judicial Conference elected to membership on the Board of the Federal Judicial Center, each for a term of four years, Chief Bankruptcy Judge Robert F. Hershner, Jr. of the Middle District of Georgia to replace Bankruptcy Judge A. Thomas Small, and Magistrate Judge Robert B. Collings of the District of Massachusetts to replace Magistrate Judge Virginia M. Morgan.

EXECUTIVE COMMITTEE

FINANCIAL DISCLOSURE LEGISLATION

The authority to redact information from financial disclosure reports when the release of such information could endanger a judge or judicial employee was granted to the Judicial Conference by the Identity Theft and Assumption Deterrence Act of 1998 (Public Law No. 105-318), which modified section 105(b) of the Ethics in Government Act of 1978 (5 U.S.C. app. § 105(b)). However, this grant of authority is scheduled to expire on December 31, 2001. On recommendation of the Committee on Financial Disclosure, concurred in by the Committee on Security and Facilities, the Executive Committee determined, on behalf of the Judicial Conference, that the judiciary should take prompt action to seek the elimination of the sunset provision found in section 7 of the Identity Theft and Assumption Deterrence Act (5 U.S.C. app. § 105(b)(3)(E)).

FEDERAL COURTS IMPROVEMENT BILL

Every two years, each Conference committee considers legislative initiatives within its jurisdiction that were approved by the Conference but not

yet enacted to decide whether those provisions should be pursued in the upcoming federal courts improvement bill, and notifies the Executive Committee of its determinations. At its February 2001 meeting, the Executive Committee reviewed the positions of the committees on whether pending Conference positions should be pursued in the 107th Congress. With two exceptions (which were referred back to the relevant committees for further consideration), the Executive Committee concurred in the determinations of the committees to include or not to include these provisions in the bill.

The Executive Committee also reviewed a legislative provision within its own jurisdiction that had not been enacted and the pursuit of which had previously been suspended by the Committee since its enactment was unlikely. This provision would establish a Judicial Conference Foundation to receive and expend private contributions in support of official programs (JCUS-MAR 95, p. 6). The Committee determined to continue to defer pursuit of such a foundation.

MISCELLANEOUS ACTIONS

The Executive Committee—

- Agreed to adjust for inflation the alternative subsistence rate for judges itemizing travel expenses and to reinstate the annual automatic inflation adjustment to that rate, subject to Executive Committee review;
- Supported the Financial Disclosure Committee's adoption of a standard for granting waivers of the fee for obtaining copies of financial disclosure reports (i.e., a demonstrated inability to pay), and the application of that standard to deny a waiver for a media organization requesting the 1999 financial disclosure reports of all Article III judges;
- Received a report of the Magistrate Judges Committee on the growth of the magistrate judges system;
- Asked the Committee on the Administrative Office to undertake a review of reports required by law to be produced by the Administrative Office;

- Approved a resolution honoring Representative Harold Rogers, former Chairman of the House Appropriations Subcommittee on the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies; and
- Agreed on the need for prompt action to minimize any non-business related activity that is being conducted on court computers; determined to encourage all chief judges to establish policies in their courts on the appropriate use of the Internet; and asked the Committee on Automation and Technology to continue current efforts in information technology (IT) security and to develop a comprehensive plan for improving IT security in the courts.

COMMITTEE ON THE ADMINISTRATIVE OFFICE

WIRETAP REPORTS

The Omnibus Crime Control and Safe Streets Act of 1968 requires the Administrative Office to report to Congress annually the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral or electronic communications (“wiretap orders”) based on reports submitted to the agency by federal and state judges and prosecutors (18 U.S.C. § 2519(1), (2), and (3)). In March 1992, the Judicial Conference determined to seek legislation to have this responsibility transferred to the United States Department of Justice (JCUS-MAR 92, p. 14), but has been unable to win sufficient support in Congress to accomplish this end. In an effort to simplify the process, at this session, the Conference approved an Administrative Office Committee recommendation that the judiciary seek an amendment to 18 U.S.C. § 2519(1) to allow judges to submit a single annual report to the Administrative Office, no later than January of each year, that reports on all wiretap orders for the preceding calendar year rather than an individual report each time a wiretap order is approved or denied. This change would reduce the burden on the judges and their staffs without impacting the accuracy or timeliness of the AO’s report, and would not be mandatory for judges who wish to continue submitting reports throughout the year.

COMMITTEE ACTIVITIES

The Committee on the Administrative Office reported that it reviewed the status of several major initiatives and studies undertaken by the Administrative Office. The Committee was briefed on the AO's investigative assistance to the courts in resolving allegations against judiciary employees or others having business with the courts, and on how the judiciary's administrative oversight mechanisms had been used effectively to identify potential irregularities in the courts. The Committee endorsed oversight enhancement initiatives, including a handbook for chief judges and programs that increase chief judges' awareness of administrative management and internal control issues. The Committee also received a comprehensive briefing on the Administrative Office's human resources initiatives, including the success of new benefits programs and efforts to seek legislation that would provide the Director of the Administrative Office with independent benefits authority; the successful implementation of the new Human Resources Management Information System in the Administrative Office, the Federal Judicial Center, and the U.S. Sentencing Commission, and plans to expand the system to the courts; and implementation of new staffing formulae in the courts.

COMMITTEE ON AUTOMATION AND TECHNOLOGY

LONG RANGE PLAN FOR INFORMATION TECHNOLOGY

Pursuant to 28 U.S.C. § 612 and on recommendation of the Committee on Automation and Technology, the Judicial Conference approved the 2001 update to the *Long Range Plan for Information Technology in the Federal Judiciary*. Funds for the judiciary's information technology program must be spent in accordance with this plan.

LOCATION OF COURT RECORDS

Section 457 of title 28, United States Code, requires that the "records of district courts and courts of appeals shall be kept at one or more of the places where court is held." However, for electronic records, developments in computer and network technology have virtually eliminated physical location

of the hardware on which such records reside as a factor in accessing those records, and the ability to store information electronically in multiple locations dramatically reduces potential loss from manmade or natural disasters. On recommendation of the Committee on Automation and Technology, the Judicial Conference agreed to seek a legislative change to 28 U.S.C. § 457 to delete any reference to physical location requirements so as to accommodate electronic records and supporting repositories.

COMMITTEE ACTIVITIES

The Committee on Automation and Technology reported that it had received the results of a comprehensive, independent study of the judiciary's national information technology program, which concluded that the judiciary has established a national information technology program using significantly fewer resources than other government organizations. The Committee also discussed Internet and electronic mail traffic and requested further analysis; reviewed progress in an ongoing study of lawbooks and libraries; and received updates on a number of other information technology projects and issues, such as implementation of the new case management/electronic case files system and new technologies for obtaining remote access to the judiciary's data communications network.

COMMITTEE ON THE ADMINISTRATION OF THE BANKRUPTCY SYSTEM

REAPPOINTMENT OF BANKRUPTCY JUDGES

In March 1997, the Judicial Conference added a chapter to the selection and appointment regulations for bankruptcy judges (chapter 5) to provide for reappointment of incumbent bankruptcy judges without subjecting them to the full application and merit screening process required of candidates for new positions (JCUS-MAR 97, p. 13). Chapter 5 was subsequently amended to address appellate court concerns with certain time frames set forth in those regulations (JCUS-SEP 00, pp. 43-44). At this session, on recommendation of

the Committee on the Administration of the Bankruptcy System,² the Judicial Conference made additional changes to chapter 5 to (a) clarify that a court of appeals will consider an incumbent bankruptcy judge who seeks reappointment before considering other qualified candidates; (b) remove a phrase from section 5.01(b) that might appear to create a presumption of reappointment; (c) empower the chief judge of a court of appeals to extend time periods set forth in the reappointment regulations, rather than requiring a vote of the active members of that court; (d) eliminate a requirement in section 5.01(c) that the court of appeals take an initial vote to determine whether the incumbent appears to merit reappointment, and provide that the court of appeals proceed directly to the public comment period; and (e) extend from 30 to 60 days the time period during which the court of appeals must vote on the reappointment following receipt of public comment.

PLACE OF HOLDING BANKRUPTCY COURT

On the recommendation of the Bankruptcy Committee, and in accordance with 28 U.S.C. § 152(b)(1), the Judicial Conference approved the request of the Western District of Missouri and the Eighth Circuit Judicial Council to designate Carthage, Missouri, as an additional place of holding bankruptcy court in the Western District of Missouri, and delete the designation of Joplin, Missouri.

COMMITTEE ACTIVITIES

The Bankruptcy Committee reported that it addressed several fee issues. It proposed to the Court Administration and Case Management Committee, for recommendation to the Conference, an amendment to the Bankruptcy Court Miscellaneous Fee Schedule to provide that fees for appeals or cross-appeals by bankruptcy trustees (and debtors in possession in chapter 11 cases) be payable only from the estate and to the extent that an estate is realized, in order to encourage trustees to pursue estate assets. The Committee also concurred in the recommendations of the Committee on Court Administration and Case Management with regard to the revision and restructuring of electronic public

² The Bankruptcy Committee's original recommendations were revised prior to the Judicial Conference session in response to concerns raised by the Executive Committee.

access fees, and it endorsed other amendments to the Bankruptcy Miscellaneous Fee Schedule (*see infra* “Miscellaneous Fee Schedules,” pp. 12-15).

COMMITTEE ON THE BUDGET

TRANSFER OF RETIREMENT FUNDS

The Judicial Conference adopted a recommendation of the Budget Committee that the Conference rescind its March 1993 decision to pursue legislation that would allow the judiciary’s contributions to the Civil Service Retirement Fund to be returned to the judiciary when bankruptcy and magistrate judges for whom the benefits are paid elect to transfer out of the Civil Service Retirement System (JCUS-MAR 93, p. 6). The proposal has been rejected by the last four Congresses, and there is little likelihood of its enactment.

COMMITTEE ACTIVITIES

The Committee on the Budget reported that it discussed efforts to establish a greater linkage between the annual budget formulation process and the use of the long-range budget estimates. To assist the Committee in these efforts, the Administrative Office will develop long-range budget estimates in the fall of each year rather than in the spring. This change will enable the Budget Committee to review updated estimates at its January meetings and use these estimates in preparing the budget guidance to the program committees for the following spring/summer budget cycles. The Committee also discussed strategies for presenting the 2002 budget request to Congress and the need to emphasize the quality of justice when justifying annual requests for resources.

COMMITTEE ON CODES OF CONDUCT

CODE OF CONDUCT FOR JUDICIAL EMPLOYEES

Canon 3F(4) of the Code of Conduct for Judicial Employees requires certain designated employees to keep informed of their own and their close

relatives' financial interests in order to avoid conflicts of interest. The Committee on Codes of Conduct recommended amending Canon 3F(4) to add a definition of "financial interest" and to clarify that judicial employees have no duty to inquire about relatives' fiduciary interests. These amendments would conform the "duty of inquiry" provisions for judicial employees to the corresponding provisions applicable to judges under Canon 3C(2) of the Code of Conduct for United States Judges (*see* JCUS-SEP 99, p. 52). The Committee also proposed limiting application of Canon 3F(4) to the employees specified in Canon 3F(2)(a) (i.e., law clerks and staff attorneys), as these are the only employees who, like judges, are subject to automatic disqualification due to financial interest. The Conference approved the amendments to Canon 3F(4), which read as follows (new language is in italics; deleted language is struck through):

(4) A judicial employee who is subject to Canon 3F(2)(a) should keep informed about his or her personal, ~~financial~~ and fiduciary *financial* interests and make a reasonable effort to keep informed about ~~such~~ *the personal financial* interests of a spouse or minor child residing in the judicial employee's household. *For purposes of this canon, "financial interest" means ownership of a legal or equitable interest, however small, or a relationship as director, advisor, or other active participant in the affairs of a party, except that:*

(i) ownership in a mutual or common investment fund that holds securities is not a "financial interest" in such securities unless the employee participates in the management of the fund;

(ii) an office in an educational, religious, charitable, fraternal, or civic organization is not a "financial interest" in securities held by the organization;

(iii) the proprietary interest of a policy holder in a mutual insurance company, or a depositor in a mutual savings association, or a similar proprietary interest, is a "financial interest" in the organization only if the outcome of the proceeding could substantially affect the value of the interest;

(iv) ownership of government securities is a “financial interest” in the issuer only if the outcome of the proceeding could substantially affect the value of the securities.

COMMITTEE ACTIVITIES

Since its last report in September 2000, the Committee on Codes of Conduct received 25 new written inquiries and issued 26 written advisory responses. During this period, the average response time for requests was 19 days. The Chairman received and responded to 23 telephonic inquiries. In addition, individual Committee members responded to 135 inquiries from their colleagues.

COMMITTEE ON COURT ADMINISTRATION AND CASE MANAGEMENT

MISCELLANEOUS FEE SCHEDULES

Electronic Public Access. Pursuant to 28 U.S.C. §§ 1913, 1914, 1926(a), 1930(b) and 1932, the Judicial Conference is authorized to prescribe fees to be collected by the appellate and district courts, the Court of Federal Claims, the bankruptcy courts, and the Judicial Panel on Multidistrict Litigation, respectively. While the various fees included in these miscellaneous fee schedules are often court-specific, the fees pertaining to electronic public access (EPA) to court information cut across fee schedule lines. The Judicial Conference approved a Court Administration and Case Management Committee recommendation that EPA fees be removed from the various courts’ fee schedules and reissued in an independent miscellaneous EPA fee schedule that would apply to all court types.

The Committee also recommended three substantive amendments to the EPA fee schedule. The first amendment concerned the user fee for Internet access to the judiciary’s new case management/electronic case files (CM/ECF) system. Pursuant to section 404 of Public Law No. 101-515, which directs the Judicial Conference to prescribe reasonable fees for public access to information available in electronic form, the judiciary established a seven cents per page fee for Internet access to electronic court records that will apply to CM/ECF when it is introduced (JCUS-SEP 98, p. 64). In response to

concerns about the effect of these fees on open access to court records, especially with regard to litigants, the Committee recommended that the schedule be amended to state that attorneys of record and parties in a case (including pro se litigants) receive one free electronic copy of all filed documents, if receipt is required by law or directed by the filer, which could then be printed and saved to the recipient's own computer or network. The Committee further recommended that no fee under this provision be owed until an individual account holder accrued charges of more than \$10 in a calendar year. This would allow free access to over 140 electronic pages, providing a basic level of public access consistent with the services historically provided by the courts. After discussion, the Conference adopted the Committee's recommendations.

The Committee's second proposal was for the establishment of a new fee of 10 cents per page for printing paper copies of documents through public access terminals at clerks' offices. This proposed fee, set at a level commensurate with the costs of providing existing services and developing enhanced services, is less than the 50 cents per page fee currently being charged for retrieving and copying court records and would therefore encourage the use of public access terminals and reduce demands on clerks' offices. The Conference approved the Committee's recommendation.

Lastly, the Committee recommended, and the Conference approved, the establishment of a Public Access to Court Electronic Records (PACER) Service Center search fee of \$20. The PACER Service Center provides registration, billing, and technical support for the judiciary's EPA systems and receives numerous requests daily for particular docket sheets from individuals who do not have PACER accounts. This fee would be consistent with the fees currently imposed "for every search of the records of the court, and for certifying the results thereof" in the other fee schedules.

Reproduction of Recordings. The miscellaneous fee schedules for the appellate, district, and bankruptcy courts include a provision requiring that a fee be charged for "reproduction of magnetic tape recordings, either cassette or reel-to-reel...including the cost of materials." The Committee recommended that this fee be modified to account for the expanded variety of media technologies, including the use of digital equipment, rather than magnetic tape recordings. In addition, the Committee recommended that the current exemption from the fee for the federal government be eliminated when the requested record is available through the judiciary's CM/ECF system. Approving the Committee's recommendations, the Conference amended

Item 5 of the appellate and district court miscellaneous fee schedules and Item 3 of the bankruptcy court miscellaneous fee schedule relating to the reproduction of recordings to read as follows:

For reproduction of recordings of proceedings, regardless of the medium, \$20, including the cost of materials. This fee shall apply to services rendered on behalf of the United States, if the reproduction of the recording is available electronically.

The Conference also agreed to amend the preambles to the appellate, district, and bankruptcy court miscellaneous fee schedules to eliminate the exemption for federal agencies from the fee for reproduction of recordings.

Local Rules. The Conference adopted a Committee recommendation to amend provisions in the appellate, district, and bankruptcy court and Court of Federal Claims miscellaneous fee schedules (Item 11, Item 12, Item 18, and Item 6, respectively) to reflect that local rules may be provided by means other than printing a paper copy, such as electronically via the Internet. The provisions were amended as follows (new language is in italics; deleted language is struck through):

The court may charge and collect fees, ~~commensurate with the cost of printing,~~ for copies of the local rules of court *commensurate with the cost of providing such copies.* The court may also distribute copies of the local rules without charge.

Amendments in Bankruptcy Cases. On recommendation of the Committee, the Conference amended Item 4 of the Bankruptcy Court Miscellaneous Fee Schedule, which prescribes a fee of \$20 for each amendment to a debtor's schedules of creditors or lists of creditors, to make clear that amendments to the matrices or to the mailing lists of creditors, which are often used by clerks' offices to notify creditors and other parties of actions relating to the bankruptcy case, would also generate the \$20 fee. This provides an incentive to debtors to make certain that matrices and mailing lists are accurate when filed.

Miscellaneous Documents. Both the district and the bankruptcy court miscellaneous fee schedules impose a fee for filing or indexing a miscellaneous document not in a case or proceeding for which a filing fee has been paid, except that the district court provision sets forth four specific

instances in which the fee is applicable while the bankruptcy court provision is more general. For consistency, the Judicial Conference, on recommendation of the Committee, amended both Item 1 of the District Court Miscellaneous Fee Schedule and Item 7 of the Bankruptcy Court Miscellaneous Fee Schedule to read as follows:

For filing or indexing any document not in a case or proceeding for which a filing fee has been paid, \$30.

CIVIL LITIGATION MANAGEMENT MANUAL

On recommendation of the Committee and as required by the Civil Justice Reform Act of 1990 (CJRA) (*see* 28 U.S.C. § 479(c)(1)), the Judicial Conference approved for publication a civil litigation management manual that describes those litigation management and cost and delay reduction principles, techniques, and programs deemed most effective by the Judicial Conference and the Directors of the Administrative Office and the Federal Judicial Center.

JUROR QUALIFICATION QUESTIONNAIRE

In September 2000, the Judicial Conference revised the juror qualification questionnaire to conform the categories on race and ethnicity to those used by the Census Bureau for the 2000 census (JCUS-SEP 00, pp. 47-48). The Census Bureau and other executive branch agencies have since revised the terminology used to describe some of those categories. Specifically, the term “Black” has been changed to “Black or African American”; the term “Hispanic” has been changed to “Hispanic or Latino”; and the term “Native American Indian” has been changed to “American Indian or Alaska Native.” So that the juror qualification questionnaire terminology will continue to mirror that used by the Census Bureau, the Conference approved a Committee recommendation that Question 10 of the juror qualification questionnaire be revised to incorporate these changes.

SOCIAL SECURITY REPORTING REQUIREMENTS

Social security appeals are included in the Civil Justice Reform Act statistical reports in the same way as motions in civil cases, but with a pending

date from which the six-month clock begins to run set at 120 days after the filing of the transcript in the case (JCUS-SEP 98, p. 63; JCUS-SEP 99, p. 58). A small number of courts have adopted procedures that have the effect of delaying by up to two months the date from which the clock begins to run by allowing the transcript to be filed with the court when the Commissioner of Social Security files the responsive brief, rather than when the transcript is served on the claimant. These procedures are similar to the “holding” procedures for civil motions discussed by the Conference in September 1999 (JCUS-SEP 99, pp. 57-58), in that they raise concerns about the uniformity of the reporting requirements and about compliance with Rule 5(d) of the Federal Rules of Civil Procedure (which requires all papers served upon a party to be filed with the court “within a reasonable time after service”). On recommendation of the Committee, the Conference agreed to amend the instructions for the CJRA report on social security appeals pending over six months, as published in the *Guide to Judiciary Policies and Procedures*, to define the “pending date” for such appeals to be reported as 120 days after the filing of the transcript in the case, or in cases where the transcript is served upon a party before it is filed with the court, then 120 days after the initial service of the transcript. The Conference further agreed to request that each circuit council review local rules with “holding” procedures for social security cases to ensure compliance with Federal Rule of Civil Procedure 5(d).

COMMITTEE ACTIVITIES

The Committee on Court Administration and Case Management reported on a number of issues relating to electronic case filing, including the Committee’s extensive work on a judiciary-wide privacy policy for consideration by the Conference, and its evaluation of existing local court rules and practices pertaining to electronic filing. In other areas, the Committee provided its views on courtroom sharing for magistrate and bankruptcy judges to the Committee on Security and Facilities; considered the development of processes for identifying and assisting “high workload courts,” as recommended by the Judicial Officers Resources Working Group; and began consideration of the issue of the changing nature of litigation in the district courts.

COMMITTEE ON CRIMINAL LAW

RISK PREDICTION INDEX

In March 1997, the Judicial Conference approved the use of the Risk Prediction Index (RPI) by probation officers to assist in the assessment of the risk of recidivism posed by offenders being supervised on terms of probation and supervised release (JCUS-MAR 97, p. 21). Studies conducted by the Federal Judicial Center, at the request of the Criminal Law Committee, demonstrate that the RPI can also be useful in identifying those individuals released to pretrial services supervision who are likely to succeed and those who are likely to have their release status revoked. Accordingly, the Committee recommended, and the Judicial Conference approved, the use of the Risk Prediction Index by pretrial services officers (and probation officers in combined districts) to assist in the assessment of risk posed by defendants under pretrial services supervision.

JUDGMENTS IN A CRIMINAL CASE

On the Committee's recommendation and after discussion, the Conference approved revised forms for judgments in a criminal case (AO 245B-AO 245I) for publication and distribution to the courts. The judgment forms were revised to include express language indicating adjudication of guilt. In addition, in order to protect the identity of cooperating defendants, the portion of the forms entitled "Statement of Reasons," which includes sensitive information about whether a defendant's substantial assistance served as the basis for a sentence departure, was revised to become an attachment to the judgment forms, and will not be disclosed to the public. However, the complete judgment form, including the Statement of Reasons, will continue to be forwarded to appropriate entities, such as the United States Sentencing Commission, the Federal Bureau of Prisons, defense counsel, government attorneys, and the appellate courts.

COMMITTEE ACTIVITIES

The Committee on Criminal Law reported on the status of a strategic assessment of the probation and pretrial services system and on the activities of an ad hoc work group that is reviewing and revising the pretrial services

and post-conviction supervision monographs. The Committee also reviewed a report on an independent study of the federal judiciary's home confinement program, which will be published and disseminated to the courts later this year.

COMMITTEE ON DEFENDER SERVICES

COMMUNITY DEFENDER ORGANIZATION GRANT AND CONDITIONS AGREEMENT

On recommendation of the Defender Services Committee, the Judicial Conference approved revisions to clause 8 of the grant and conditions agreement to prohibit community defender organizations (CDOs) from using Criminal Justice Act (CJA) grant funds to contract locally for audit services that would duplicate the AO's national contract audit. The revisions would also require prior approval of the AO's Defender Services Division before a CDO may use grant funds to engage an expert to respond to findings of a national contract audit. The fourth paragraph of clause 8 was amended to read as follows (new language is in italics):

The grantee may contract with local accountants or with the Auditor, for any accounting and financial services necessary for the operation of its office, including, but not limited to, the preparation of all required federal and state tax returns and any additional annual audit reports required by the Board of Directors *that do not duplicate the national contract audit. Notwithstanding the foregoing, a grantee may use grant funds to contract with an expert for the purpose of responding to a finding of the Auditor in the annual audit when authorized in advance to do so by the Defender Services Division.*

REASONABLE ACCOMMODATION FOR EMPLOYEES WITH DISABILITIES

Section 3102 of title 5, United States Code, as recently amended by section 311 of Public Law No. 106-518, the Federal Courts Improvement Act of 2000, authorizes the head of each agency in the judicial branch to provide personal assistants for disabled judges or employees, as determined necessary

by the agency head. In order to implement this legislation with respect to federal defender organizations, the Committee on Defender Services recommended that the Judicial Conference take the following actions:

- a. Designate federal public defenders as “agency heads” for purposes of appointing personal assistants for individuals with disabilities in federal public defender organizations;
- b. Provide executive directors of community defender organizations with the same authority as federal public defenders with respect to individuals with disabilities in those organizations; and
- c. Authorize the Administrative Office to develop guidelines for federal public defenders and executive directors of community defender organizations to use in determining when and in what circumstances the creation of a personal assistant position is appropriate.

The Conference adopted the Committee’s recommendations. *See also infra*, “Reasonable Accommodation for Employees with Disabilities,” pp. 25-26.

PROFESSIONAL LIABILITY INSURANCE

The judiciary’s fiscal year 1999 appropriations act (Public Law No. 105-277), as amended by Public Law No. 106-58, requires the judiciary to reimburse judges and certain judicial employees for up to half the cost of professional liability insurance. The guidelines adopted by the Judicial Conference to implement this program for federal public defender organization (FPDO) employees (JCUS-SEP 99, pp. 61-62; JCUS-MAR 00, p. 7), placed a \$150 cap on the amount of reimbursement an eligible individual was entitled to receive. Due to an increase in premiums, the Committee on Defender Services recommended that the guidelines for FPDO employees be amended to lift the \$150 cap and permit reimbursement of up to one-half the cost of the policy, regardless of the dollar amount. The Judicial Conference approved the recommendation. *See also infra* “Professional Liability Insurance,” p. 26.

AMICUS CURIAE POLICY FOR FEDERAL DEFENDERS

On recommendation of the Committee on Defender Services, the Judicial Conference approved the addition of a new paragraph to Chapter IV (“Defender Organizations”) of the Guidelines for the Administration of the Criminal Justice Act and Related Statutes (CJA Guidelines), which sets forth the circumstances in which federal defenders may participate as *amicus curiae* in CJA cases. The new section formalizes a longstanding practice of permitting federal defenders to participate as *amicus curiae* when requested to do so by an appellate court, and in death penalty habeas corpus cases. The section further authorizes federal defenders to participate as *amicus curiae* in cases where, in the defender’s judgment, a legal issue affects the case of a client whom the defender represents, i.e., “on behalf of a client as an ancillary matter appropriate to the proceedings.” See 18 U.S.C. § 3006A(c). The new paragraph reads as follows:

4.06 Participation as *Amicus Curiae*. Pursuant to governing court rules, Federal Public Defenders and Community Defenders may participate as *amicus curiae* in federal court at the invitation of the court, in death penalty habeas corpus cases, or on behalf of a client as an ancillary matter appropriate to the proceedings.

USE OF CJA RESOURCES

In an effort to provide specific guidance on the use of CJA resources by panel attorneys for automation-related needs involving unusual or extraordinary expenses, the Defender Services Committee recommended, and the Conference approved, a revision to paragraph 3.16 of the CJA Guidelines. The revision requires, among other things, that panel attorneys consult with the Defender Services Division prior to requesting court authorization to use CJA funds to acquire computer hardware or software costing more than \$300, or to obtain computer systems and automation litigation support personnel and experts whose services are expected to have a combined cost exceeding \$10,000, and that any computer hardware or software acquired with CJA funds remains the property of the United States. The Conference also approved a model order, to be included in Appendix C (“Advance

Authorization”) of the CJA Guidelines, for authorizing the acquisition of computer hardware and/or software in conformance with the revised guideline.

COMMITTEE ACTIVITIES

Under its delegated authority from the Judicial Conference (JCUS-MAR 89, pp. 16-17), the Committee on Defender Services approved fiscal year 2001 budgets for 56 federal public defender organizations totaling \$210,417,000, and for 15 community defender organizations in the total amount of \$57,960,400.

The Committee on Defender Services reported that it met with the Chairman of the Budget Committee to discuss budgetary matters, with particular attention to the judiciary’s request for FY 2002 funding for a \$113 hourly panel attorney rate, as approved by the Conference in September 2000 (JCUS-SEP 00, pp. 44-45; 50). The Committee continued its strategic planning effort by examining fundamental aspects of the Defender Services program from a broad-based perspective.

COMMITTEE ON FEDERAL-STATE JURISDICTION

RESIDENT ALIEN PROVISOR

The Committee on Federal-State Jurisdiction identified a need to amend the "resident alien proviso" in section 1332(a) of title 28, United States Code, to clarify the scope of diversity of citizenship jurisdiction in disputes involving aliens admitted to the United States as permanent residents. Congress added this proviso to the section in 1988 to "deem" an alien admitted for permanent residence as a citizen of the state in which the alien is domiciled with the specific purpose of denying federal jurisdiction in suits between a citizen of a state and an alien permanently residing in the same state. However, the proviso's deeming language has been interpreted as applying to other litigation circumstances involving aliens. For example, under section 1332(a)(2), a non-resident alien has been permitted to sue a United States citizen and a resident alien by deeming the resident alien to be a citizen of the state of his domicile. Such application of the proviso has broadened the scope of diversity jurisdiction beyond that contemplated when the statute was enacted. Thus, upon recommendation from the Committee on

Federal-State Jurisdiction, the Judicial Conference agreed to propose legislation to resolve conflicting interpretations of the resident alien proviso in 28 U.S.C. § 1332(a) by deleting that proviso and substituting therefor text providing that the district courts shall not have diversity of citizenship jurisdiction under subsections 1332(a)(2)-(3) where the matter in controversy is between a citizen of a state and a citizen or subject of a foreign state admitted to the United States for permanent residence and domiciled in the same state.

COMMITTEE ACTIVITIES

The Committee on Federal-State Jurisdiction reported on its continuing assessment of legislative proposals that would, among other things, permit individuals in federal and state custody to request post-conviction DNA testing and provide a system for ensuring competent counsel in the states for indigent defendants in capital cases. The Committee also informed the Conference of its consideration of mass torts/class action issues, attorney conduct rules in the federal courts, the Committee's project to ascertain amendments for jurisdictional improvements, and the Federal Judicial Code Revision Project of the American Law Institute.

COMMITTEE ON FINANCIAL DISCLOSURE

COMMITTEE ACTIVITIES

The Committee on Financial Disclosure reported that as of December 31, 2000, the Committee had received 3,521 financial disclosure reports and certifications for the calendar year 1999, including 1,285 reports and certifications from Supreme Court Justices, Article III judges, and judicial officers of special courts; 365 from bankruptcy judges; 509 from magistrate judges; and 1,362 from judicial employees.

COMMITTEE ON INTERCIRCUIT ASSIGNMENTS

COMMITTEE ACTIVITIES

The Committee on Intercircuit Assignments reported that during the period from July 1, 2000, to December 31, 2000, a total of 89 intercircuit assignments, undertaken by 70 Article III judges, were processed and recommended by the Committee and approved by the Chief Justice. During calendar year 2000, a total of 190 intercircuit assignments were processed and approved. In addition, the Committee aided courts requesting assistance by both identifying and obtaining judges willing to take assignments.

COMMITTEE ON INTERNATIONAL JUDICIAL RELATIONS

COMMITTEE ACTIVITIES

The Committee on International Judicial Relations reported on its involvement in rule-of-law and judicial reform activities relating to Africa, Asia, Europe, and Latin America, including United States Agency for International Development-funded programs to build upon the already-established partnership between the Russian and U.S. judiciaries, and a presentation to the European Court of Human Rights on appellate court structure, case management, and rules. The Committee is also working with the Library of Congress' Russian Leadership Program, which brings policymakers and leaders from the Russian Federation to communities throughout the United States, in developing a rule-of-law component that will provide Russian judges an opportunity to obtain an appreciation for the United States judicial system and the role of judges in American society.

COMMITTEE ON THE JUDICIAL BRANCH

JUDICIAL COMPENSATION

The value of federal judges' salaries continues to decline due to the combination of the denial of many annual Employment Cost Index (ECI) adjustments and inflation. At the same time, the salaries of private sector lawyers and law school deans have skyrocketed. This pay erosion and pay disparity have a negative effect on judges' morale, recruitment, and retention

and represent a real threat to Article III’s guarantees of judicial independence, lifetime tenure, and undiminished compensation. Accordingly, the Judicial Conference modified slightly and then unanimously approved a Judicial Branch Committee recommendation that the Conference pursue vigorously—

- a. An Employment Cost Index adjustment for federal judges, Members of Congress, and top officials in the executive branch for 2002 and subsequent years, as provided by law;
- b. Legislation to give judges and other high level federal officials a “catch-up” pay adjustment of 9.6 percent to recapture Employment Cost Index adjustments previously foregone; and
- c. Appointment of a presidential commission to consider and make recommendations to the President on appropriate salaries for high-level officials in all three branches of government.

COMMITTEE ACTIVITIES

The Committee on the Judicial Branch reported that it has continued to devote its attention to securing salary relief for all federal judicial officers. The Committee received an update on developments in the judiciary’s benefits program and on the status of two cases raising issues concerning taxation of judicial compensation.

COMMITTEE ON JUDICIAL RESOURCES

BIENNIAL SURVEY OF JUDGESHIP NEEDS

As part of the Biennial Survey of Judgeship Needs, workloads in district and appellate courts with low weighted caseloads are reviewed for the purpose of determining whether to recommend that an existing or future judgeship vacancy not be filled. Through this process, in March 1999, the Judicial Conference recommended to the President and the Senate that an existing or future judgeship vacancy not be filled in the District Courts for the District of Columbia, the District of Delaware, the Southern District of West Virginia, and the District of Wyoming (JCUS-MAR 99, pp. 22-23). After conducting the 2001 judgeship needs survey, the Committee on Judicial Resources determined that either the caseload or the courts’ resources in the

District of Delaware and the Southern District of West Virginia had changed sufficiently to support a recommendation that any future vacancy in those courts be filled. On recommendation of the Committee, the Judicial Conference voted to amend its March 1999 position to delete the District of Delaware and the Southern District of West Virginia from the list of courts in which a vacancy should not be filled.

REASONABLE ACCOMMODATION FOR EMPLOYEES WITH DISABILITIES

As previously noted with respect to federal defender offices (*see supra* “Reasonable Accommodation for Employees with Disabilities,” pp. 18-19), the Federal Courts Improvement Act of 2000 gives the judiciary the authority to use appropriated funds to hire personal assistants for judges and employees with disabilities. Under this legislation, which amends 5 U.S.C. § 3102, the head of each agency in the judicial branch may provide for personal assistants that the agency head determines are necessary to enable a disabled judge or employee to perform his or her official duties. On recommendation of the Committee on Judicial Resources, the Judicial Conference took the following actions to implement this new law with respect to judicial officers and court employees:

- a. Approved creation of a personal assistant position under the Judiciary Salary Plan and the Court Personnel System to provide appropriate work assistance, as needed, to judges and judiciary employees with disabilities;
- b. Endorsed the Administrative Office’s use of classification flexibility currently existing under the Judiciary Salary Plan to classify personal assistant positions appropriately;
- c. Designated each chief judge, or the chief judge’s designee, as the “agency head” for judges and chambers staff, and each court unit executive as the “agency head” for employees of that unit, for purposes of appointing personal assistants for individuals with disabilities;
- d. Authorized use of central funding for personal assistant positions, as necessary, under the Judiciary Salary Plan for support of eligible judges and chambers staff;

- e. Authorized provision of an allotment to a court after receipt of a request for a personal assistant position under the Court Personnel System and an Administrative Office determination that AO guidelines were met; and
- f. Authorized the Administrative Office to develop guidelines for designated agency heads to use in determining when and in what circumstances the creation of a personal assistant position is appropriate.

PROFESSIONAL LIABILITY INSURANCE

Guidelines adopted by the Judicial Conference to implement, in accordance with Public Law No. 105-277, as amended by Public Law No. 106-58, a professional liability insurance reimbursement program for court staff (JCUS-SEP 99, pp. 66-67; JCUS-MAR 00, p. 7) placed a \$150 cap on the amount of reimbursement an eligible individual is entitled to receive. In the face of increased cost of premiums for such insurance, the Conference, on recommendation of the Committee on Judicial Resources, agreed to amend those guidelines to remove the \$150 cap, retroactive to October 1, 1999 (*see also supra*, “Professional Liability Insurance,” p. 19).

RECRUITMENT AND RETENTION BONUSES

In March 1999, the Judicial Conference authorized the use of recruitment and retention bonuses for automation positions in the courts on a two-year pilot basis (JCUS-MAR 99, p. 27). Based on findings that the program fulfills a genuine need in the courts and is being used judiciously, the Committee recommended, and the Judicial Conference agreed, that the program be made permanent.

LAW CLERK STUDENT LOANS

In September 1988, the Judicial Conference agreed to seek an amendment to 20 U.S.C. § 1077(a)(2)(C) to include full-time judicial law clerks among those occupations entitled to defer repayment, during service, of the principal on federally insured educational loans (JCUS-SEP 88, p. 90). At this session, on recommendation of the Committee, the Conference slightly

modified its September 1988 position. It determined to seek legislation deferring interest *as well as* principal on such loans during the clerkship, for a period not to exceed three years of service.

COMMITTEE ACTIVITIES

The Committee on Judicial Resources reported that it had asked the Administrative Office to conduct a comprehensive study, including a survey of Article III, bankruptcy, and magistrate judges, to determine if they are having difficulty recruiting and retaining highly qualified individuals to serve as law clerks, and, if so, to propose monetary and non-monetary solutions. The Committee also decided to ask the Administrative Office to undertake a comprehensive review of the Temporary Emergency Fund (TEF). The review will address such issues as whether there should be criteria for the allocation of law clerk and secretary positions to judges who need them and how to collect sufficient information regarding the use of the TEF. The Committee will coordinate this project with other Judicial Conference committees, as appropriate.

COMMITTEE ON THE ADMINISTRATION OF THE MAGISTRATE JUDGES SYSTEM

REIMBURSEMENT REGULATIONS

Regulations for the reimbursement of expenses incurred by part-time magistrate judges, adopted pursuant to 28 U.S.C. § 635(b), allow a part-time magistrate judge to claim reimbursement for salary expenses actually incurred for secretarial or clerical assistance rendered in connection with official magistrate judge duties, but do not make reference to reimbursement of support staff expenses for holidays, vacation leave, or sick leave. Noting that certain part-time magistrate judges at the higher salary levels require full-time or extensive staff support, the Committee on the Administration of the Magistrate Judges System recommended, and the Judicial Conference approved, amendments to the regulations to authorize reimbursement for holidays and annual and sick leave taken by judges' support staff, not to exceed federal employee entitlements. The revised regulations do not require reimbursement for holidays and leave, but only set upper limits for

reimbursement for those part-time magistrate judges who choose to claim reimbursement for such expenses.

CHANGES IN MAGISTRATE JUDGE POSITIONS

After consideration of the report of the Committee and the recommendations of the Director of the Administrative Office, the district courts, and the judicial councils of the circuits, the Judicial Conference approved the following changes in positions, salaries, locations, and arrangements for full-time and part-time magistrate judge positions. Changes with a budgetary impact are to be effective when appropriated funds are available.

THIRD CIRCUIT

District of New Jersey

1. Authorized an additional full-time magistrate judge position at Newark; and
2. Made no change in the number, locations, salaries, or arrangements of the other magistrate judge positions in the district.

FOURTH CIRCUIT

Middle District of North Carolina

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

Western District of Virginia

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

Northern District of West Virginia

1. Redesignated the full-time magistrate judge position at Elkins as Clarksburg or Elkins;

March 14, 2001

2. Redesignated the part-time magistrate judge position at Clarksburg as Martinsburg upon the appointment of a full-time magistrate judge at Clarksburg or Elkins; and
3. Made no other change in the number, locations, salaries, or arrangements of the magistrate judge positions in the district.

Southern District of West Virginia

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

FIFTH CIRCUIT

Western District of Louisiana

Increased the salary of the part-time magistrate judge position at Monroe from Level 4 (\$33,633 per annum) to Level 3 (\$44,844 per annum).

SIXTH CIRCUIT

Western District of Michigan

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

Southern District of Ohio

1. Authorized an additional full-time magistrate judge position at Dayton; and
2. Made no change in the number, locations, or arrangements of the other magistrate judge positions in the district.

Eastern District of Tennessee

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

Western District of Tennessee

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

EIGHTH CIRCUIT

Western District of Missouri

Made no change in the number, locations, or arrangements of the magistrate judge positions in the district.

TENTH CIRCUIT

District of Wyoming

Increased the salary of the part-time magistrate judge position at Casper from Level 7 (\$5,605 per annum) to Level 6 (\$11,211 per annum).

ELEVENTH CIRCUIT

Northern District of Georgia

1. Converted the part-time magistrate judge position at Rome to full-time status;
2. Authorized one additional full-time magistrate judge position at Atlanta; and
3. Made no change in the number, locations, or arrangements of the other magistrate judge positions in the district.

COMMITTEE ACTIVITIES

The Committee on the Administration of the Magistrate Judges System reported that it discussed at length the issue of the growth of the magistrate judges system. The Committee concluded that it is appropriate for it to continue to consider requests from courts for additional magistrate judge positions and to recommend approval of those requests that meet the criteria

established by the Judicial Conference, as it has to date, and that it will continue to monitor the growth of the magistrate judges system carefully. The Committee forwarded background materials and a statement of the issues on this topic to the Executive Committee (*see supra*, “Miscellaneous Actions,” p. 5).

COMMITTEE TO REVIEW CIRCUIT COUNCIL CONDUCT AND DISABILITY ORDERS

COMMITTEE ACTIVITIES

The Committee to Review Circuit Council Conduct and Disability Orders reported that it has distributed to the courts a pamphlet containing the current version of the Illustrative Rules Governing Complaints of Judicial Misconduct and Disability and related materials that may be useful to judges and court staff in implementing the complaint procedure established by 28 U.S.C. § 372(c).

COMMITTEE ON RULES OF PRACTICE AND PROCEDURE

COMMITTEE ACTIVITIES

The Committee on Rules of Practice and Procedure reported that it approved for immediate publication proposed amendments to Rule C of the Supplemental Rules for Certain Admiralty and Maritime Claims to conform with recent legislation. The Committee's Subcommittee on Technology is working with the Committee on Court Administration and Case Management studying privacy issues that arise from electronic case filing and developing guidance for courts to implement an electronic case filing system. The Advisory Committees on Appellate, Bankruptcy, Civil, and Criminal Rules are reviewing comments from the public submitted on amendments proposed to their respective sets of rules, including most significantly a proposed comprehensive style revision of the Federal Rules of Criminal Procedure.

COMMITTEE ON SECURITY AND FACILITIES

CONSTRUCTION SUBMISSION PROCESS/ FIVE-YEAR COURTHOUSE PROJECT PLAN

For the last four fiscal years, the Office of Management and Budget has either eliminated or substantially reduced funding for courthouse construction projects in the General Services Administration portion of the President's budget requests. The Committee on Security and Facilities recommended that the Judicial Conference approve a formal courthouse construction submission process that presents the current budget-year housing requirements approved by the circuit judicial councils and the Judicial Conference in the Five-Year Courthouse Project Plan, for transmission to executive branch officials, the leadership of the House and Senate, the relevant appropriations and authorizing committee chairmen, and others deemed appropriate. The submission would not be a budget request, but a formal narrative statement of the judiciary's housing requirements to educate key legislative and executive branch decision makers about these requirements. The Judicial Conference approved the Committee's recommendation by mail ballot concluded on January 30, 2001.

At the same time, the Judicial Conference, after taking into consideration the comments of the circuit judicial councils, approved the Five-Year Courthouse Project Plan for fiscal years 2002-2006 on an expedited basis, so that it could be used to prepare the courthouse construction submission. The Conference also approved by mail ballot a related recommendation that it recognize the Eleventh Circuit Court of Appeals' critical need for additional office space to house court staff in Atlanta, Georgia. (This latter proposal is not included in the Five-Year Plan because the intended building would accommodate court staff rather than judges.)

RELEASE OF SPACE

Pursuant to 28 U.S.C. § 462(f), and on recommendation of the Committee, the Judicial Conference approved the release of space and closure of the non-resident facilities in Ada in the Eastern District of Oklahoma, and in Enid in the Western District of Oklahoma.

ERGONOMICS IN THE JUDICIAL WORKPLACE

Ergonomics is the applied science of workplace equipment design intended to maximize productivity by reducing employee fatigue and discomfort. In order to prevent work-related musculoskeletal injuries and minimize financial liability for the judiciary, the Committee on Security and Facilities, with the encouragement of the Committee on Judicial Resources, recommended that the Judicial Conference endorse the concept of ergonomics in the judicial workplace and authorize the provision of information on ergonomic assessments and the acquisition of ergonomic furniture, as local funding permits, to assist courts when addressing ergonomic issues. The Conference adopted the Committee's recommendation.

BANKRUPTCY JURY BOXES

The Committee on Security and Facilities recommended to the March 2000 Judicial Conference that the *U. S. Courts Design Guide* be amended to state that an eight-person jury box should be provided "when determined necessary," in order to clarify that jury boxes in bankruptcy courtrooms are not required in every new courthouse. At that session, the Conference voted to recommit the recommendation to the Committee so that it might obtain the views of the Committee on the Administration of the Bankruptcy System, provided that while the matter was under reconsideration, a moratorium would be imposed on the design or construction of jury boxes in new or existing bankruptcy courtrooms (JCUS-MAR 00, p. 28). The Bankruptcy Committee considered the issue and concurred in the view that bankruptcy courtrooms do not normally require a jury box unless there is a demonstrated need. The Judicial Conference approved the Security and Facilities Committee recommendations that the *Design Guide* be amended to clarify that jury boxes in bankruptcy courtrooms are not required in every new courthouse and that the March 2000 moratorium on design and construction of jury boxes in new or existing bankruptcy courtrooms be lifted.

COMMITTEE ACTIVITIES

The Committee on Security and Facilities reported that, with the strong concurrence of the Judicial Branch Committee, it had rejected an Ernst & Young facilities study recommendation that senior judges have access to a

dedicated courtroom only for the first two years of senior status and share courtrooms thereafter, in favor of the existing Judicial Conference planning assumption that permits a dedicated courtroom for a senior judge for ten years after taking senior status. The Committee endorsed a proposal that requires court security officer (CSO) contractors to designate physicians to conduct physical examinations of CSOs and directed the U.S. Marshals Service to implement CSO medical standards endorsed by the Committee in June 2000.

FUNDING

All of the foregoing recommendations that require the expenditure of funds for implementation were approved by the Judicial Conference subject to the availability of funds and to whatever priorities the Conference might establish for the use of available resources.

Chief Justice of the United States
Presiding

INDEX

Administrative Office, Committee on the, 5, 6-7

Administrative Office of the U. S. Courts

- budget formulation process, 10
- changes in magistrate judge positions, 28
- Civil Litigation Management Manual, 15
- community defender organization audits, 18
- disabled employees, personal assistants, 18-19, 25-26
- law clerk recruitment and retention survey, 27
- reports required by law, 5
- Temporary Emergency Fund (TEF), 27
- wiretap reports, 6

Amicus curiae

- policy for federal defenders, 20

Appropriations

- budget formulation process, 10
- courthouse construction, 32
- Criminal Justice Act panel attorney compensation, 21
- defender organization funding, 21

Automation (*see* information technology)

Automation and Technology, Committee on, 6, 7-8

Bankruptcy judges (*see* judges, bankruptcy)

Bankruptcy system (*see also* judges, bankruptcy)

- fees, electronic public access
 - access to court files, 12-13
 - PACER Service Center search, 13
 - paper copies, public access terminals, 13
- fees, miscellaneous
 - amendments to matrices/lists of creditors, 14
 - appeals by bankruptcy trustees, 9
 - copies of local rules, 14
 - electronic public access, 9-10, 12-13

Bankruptcy system (continued)

- filing miscellaneous documents, 14-15
- reproduction of recordings, 13-14
- jury boxes, 33
- place of holding court, 9
- reappointment regulations, 8-9

**Bankruptcy System, Committee on the Administration
of the, 8-10, 33**

Benefits

- independent benefits authority, 7
- law clerks, student loan deferral, 26-27
- professional liability insurance, 19, 26

Bonuses, recruitment and retention, 26

Budget (*see* appropriations)

Budget, Committee on the, 10, 21

Case management

- case management/electronic case files systems, 12-13, 13
- Civil Justice Reform Act of 1990, 15
- Civil Litigation Management Manual, 15
- social security appeals, 15-16

Case Management/Electronic Case Files (CM/ECF), 12-13, 13

Census Bureau, 15

Chief judges (*see* judges, chief)

Circuit councils (*see* circuit judicial councils)

Circuit judges (*see* judges, circuit)

Circuit judicial councils

- changes in magistrate judge positions, 28
- courthouse construction projects, 32
- Five-Year Courthouse Project Plan, 32
- place of holding bankruptcy court, 9
- social security cases, local rules, 16

Civil Justice Reform Act of 1990 (CJRA)

- Civil Litigation Management Manual, 15
- social security appeals reporting, 15-16
- statistical reporting, 15-16

Civil Litigation Management Manual, 15

Civil rules (*see* rules of practice and procedure)

Civil Service Retirement System, 10

CM/ECF (*see* Case Management/Electronic Case Files)

Code of Conduct for Judicial Employees, 10-12

Code of Conduct for United States Judges, 11

Codes of Conduct, Committee on, 10-12

Collings, Robert B., 4

Commissioner of Social Security, 16

Community defender organizations (*see* defender services)

Compensation

- Criminal Justice Act panel attorneys, 21
- judicial, 23-24
- recruitment and retention bonuses, 26

**Conduct and Disability Orders, Committee to Review
Circuit Council, 31**

Congress

- courthouse construction projects, 32
- courthouse construction submission process, 32
- diversity jurisdiction, 21-22
- Employment Cost Index (ECI) pay adjustment, 23-24
- federal courts improvement bill, 4-5
- judgeships, Article III, 24-25
- judicial compensation, 23-24
- Judicial Conference Foundation, 5
- law clerk student loan deferrals, 26-27
- presidential commission on salaries, 24
- resident alien proviso, 21-22
- retirement funds, judiciary contribution, 10
- wiretap reports, 6

Court administration

- case management/electronic case files systems, 12-13, 13
- Civil Justice Reform Act reporting requirements, 15-16
- Civil Litigation Management Manual, 15
- court records
 - access to electronic, 12-14
 - location, 7-8
 - PACER Service Center search fee, 13
 - paper copies, public access terminals, 13
- courtroom sharing, 16, 33-34
- electronic public access, 12-13
- electronic records, location, 7-8
- fees, 9-10, 12-15
- information technology security, 6
- Internet, appropriate use, 6
- Internet access to electronic records, 12-14
- Internet access to local rules, 14
- juror qualification questionnaire, 15
- miscellaneous fee schedules, 12-15
- miscellaneous fees, 9-10, 12-15
- place of holding bankruptcy court, 9
- social security appeals reporting requirement, 15-16

Court Administration and Case Management, Committee on, 9, 12-16, 31

Court of Federal Claims

- electronic public access fees, 12-13
- miscellaneous fees, 12-13

Court Personnel System, 25-26

Court security officers

- medical standards, 34
- physical examinations, 34

Courthouses (*see* space and facilities)

Courtrooms (*see* space and facilities)

Courts of appeals (*see also* court administration)

- court records, location, 7-8
- fees, electronic public access
 - access to court files, 12-13
 - PACER Service Center search, 13
 - paper copies, public access terminals, 13
- fees, miscellaneous
 - copies of local rules, 14
 - electronic public access, 12-13
 - reproduction of recordings, 13
- forms for judgments in a criminal case, 17
- judgeship needs survey, 24-25
- reappointment of bankruptcy judges, 8-9

Criminal Justice Act (CJA) (*see also* defender services; federal defenders)

- amicus curiae* policy for federal defenders, 20
- community defender organization audits, 18
- community defender organization grant and conditions agreement, 18
- Guidelines for the Administration of the Criminal Justice Act, 20- 21
- panel attorney automation expenses, 20-21
- panel attorney compensation, 21
- use of CJA resources, 20-21

Criminal law (*see also* probation and pretrial services system)

- judgment forms, 17
- risk prediction index, 17

Criminal Law, Committee on, 17-18

Defender services (*see also* Criminal Justice Act; federal defenders)

- community defender organization audits, 18
- community defender organization grant and conditions agreement, 18
- defender organization funding, 21
- federal defender participation as *amicus curiae*, 20
- panel attorney automation expenses, 20-21
- panel attorney compensation, 21

Defender Services, Committee on, 18-21

Department of Justice

- Federal Bureau of Prisons, 17
- United States Marshals Service, 34
- wiretap reports, 6

Design Guide (*see* U. S. Courts Design Guide)

Disabled employees, reasonable accommodation, 18-19, 25-26

District courts (*see also* bankruptcy system; court administration; magistrate judges system; probation and pretrial services system)

- changes in magistrate judge positions, 28-30
- Civil Litigation Management Manual, 15
- CJRA reporting requirements, 15-16
- court records, location, 7-8
- diversity jurisdiction, 21-22
- electronic public access to court information, 12-13
- electronic records, location, 7-8
- fees, electronic public access
 - access to court files, 12-13
 - PACER Service Center search, 13
 - paper copies, public access terminals, 13
- fees, miscellaneous
 - copies of local rules, 14
 - electronic public access, 12-13
 - filing miscellaneous documents, 14-15
 - PACER Service Center search, 13
 - paper copies through public access terminals, 13
 - reproduction of recordings, 13
- forms for judgments in a criminal case, 17
- judgeship needs survey, 24-25

District courts (continued)

- jurisdiction, 21-22
- juror qualification questionnaire, 15
- release of non-resident facilities, 32

District judges (*see* judges, district)

Diversity jurisdiction, 21-22

Electronic public access (EPA) (*see also* Internet)

- access to case files, 12-13
- case management/electronic case files systems (CM/ECF), 12-13, 13
- fees, 9-10, 12-13
- local rules, 14
- miscellaneous fee schedule, 12-13
- records, location, 7-8
- reproduction of recordings, 13-14

Employment Cost Index (ECI) pay adjustments, 23-24

Ergonomics, 33

Ernst & Young, 33-34

Ethics in Government Act of 1978, 4

Executive branch

- Census Bureau, 15
- Commissioner of Social Security, 16
- courthouse construction projects, 32
- Department of Justice, 6
 - Federal Bureau of Prisons, 17
 - United States Marshals Service, 34
- Employment Cost Index pay adjustment, 24
- General Services Administration, 32
- Office of Management and Budget, 32
- President of the United States, 24, 32
- presidential commission on salaries, 24
- race and ethnicity terminology, 15

Executive Committee, 4-6, 9, 31

Federal Bureau of Prisons, 17

Federal Courts Improvement Act of 2000, 18, 25

Federal courts improvement legislation, 4-5

Federal defenders (*see also* Criminal Justice Act, defender services)

amicus curiae policy, 20

disabled, personal assistants, 18-19

professional liability insurance, 19

Federal Judicial Center, 4, 7, 15, 17

Federal public defender organizations (*see* Criminal Justice Act, defender services)

Federal rules (*see* rules of practice and procedure)

Federal-State Jurisdiction, Committee on, 21-22

Fees

amendments in bankruptcy cases, 14

appeals by bankruptcy trustees, 9

copies, public access terminals, 13

copies of local rules, 14

electronic public access, 9-10, 12-13

filing miscellaneous documents, 14-15

financial disclosure report copies, waiver, 5

Internet access to court records, 12-13

miscellaneous, 9-10, 12-15

miscellaneous fee schedules

bankruptcy, 9-10, 12-15

court of appeals, 12-14

Court of Federal Claims, 12-13, 14

district court, 12-15

electronic public access, 12-13

Judicial Panel on Multidistrict Litigation, 12-13

PACER Service Center search, 13

reproduction of recordings, 13-14

waiver, financial disclosure report copies, 5

Financial Disclosure, Committee on, 4, 5, 22

Financial disclosure reports, 4, 5, 22

authority to redact, 4

copy fee waiver, 5

Identity Theft and Assumption Deterrence Act of 1998, 4

legislation, 4

Five-Year Courthouse Project Plan, 32

General Services Administration, 32

Guide to Judiciary Policies and Procedures, 16

**Guidelines for the Administration of the Criminal
Justice Act and Related Statutes, 20-21**

Hershner, Robert F. Jr., 4

Identity Theft and Assumption Deterrence Act of 1998, 4

Illustrative Rules Governing Complaints of Judicial Misconduct and Disability, 31

Information technology (*see also* Internet)

appropriate use, 6

electronic records, location, 7-8

Long Range Plan for Information Technology in the Federal Judiciary, 7

recruitment and retention bonuses, automation positions, 26

security, 6

use of CJA resources, 20-21

Intercircuit assignments, 23

Intercircuit Assignments, Committee on, 23

International Judicial Relations, Committee on, 23

Internet (*see also* information technology)

access to court information, 12-13

appropriate use policies, 6

case management/electronic case files, 12-13

fee for access to court records, 12-13

fee for copies of local rules, 14

non-business-related sites, 6

Judicial Conference of the United States

Judges, Article III (*see also* judges, federal; judgeships, Article III)

- compensation, 23-24
- intercircuit assignments, 23
- senior, courtroom sharing, 34

Judges, bankruptcy (*see also* bankruptcy system; judges, federal)

- courtroom sharing, 16
- reappointment, 8-9
- retirement funds, judiciary contribution, 10

Judges, chief

- appellate, reappointment of bankruptcy judges, 9
- handbook on administrative oversight, 7
- Internet, policy on appropriate use, 6
- reasonable accommodation for employees with disabilities, 25

Judges, circuit (*see* judges, Article III; judges, chief; judges, federal)

Judges, Court of Federal Claims (*see* judges, federal)

Judges, district (*see* judges, Article III; judges, chief; judges, federal)

Judges, federal (*see also* judges, Article III; judges, bankruptcy; judges, chief; judges, magistrate)

- Code of Conduct for United States Judges, 11
- compensation, 23-24
- disabled, personal assistants, 25-26
- financial disclosure, 4, 22
- pay adjustments, 23-24
- travel reimbursement rate, 5
- wiretap reports, 6

Judges, magistrate (*see also* judges, federal; magistrate judges system)

- changes in positions, 28-30
- part-time, reimbursement for certain staff expenses, 27-28
- reimbursement regulations, 27-28
- retirement funds, judiciary contribution, 10

Judgeships, Article III

- biennial survey of needs, 24-25
- eliminating or not filling, 24-25
- vacancies, 24-25

Judgments in a criminal case, 17

Judicial Branch, Committee on the, 23-24, 33

Judicial Conference of the United States

- Foundation, 5
- funding of actions, 34
- mail ballots, 32

Judicial Panel on Multidistrict Litigation

- electronic public access fees, 12-13

Judicial Resources, Committee on, 24-27, 33

Judiciary Salary Plan, 25

Jury administration

- juror qualification questionnaire, 15
- jury boxes in bankruptcy courtrooms, 33

Law clerks

- code of conduct, 10-12
- conflict of interest, duty of inquiry, 10-12
- recruitment and retention survey, 27
- student loan deferral, 26-27

Legislative branch (*see* Congress)

Local rules, 14, 16

Long Range Plan for Information Technology in the Federal Judiciary, 7

Magistrate judges (*see* judges, magistrate)

Magistrate judges system (*see also* judges, magistrate)

- changes in positions, 28-30
- courtroom sharing, 16
- growth, 5, 30-31
- part-time judges, reimbursement for certain staff expenses, 27-28
- reimbursement regulations, 27-28

Magistrate Judges System, Committee on the Administration of the, 5, 27-31

Mail ballots of the Judicial Conference

- courthouse construction submission process, 32
- five-year courthouse project plan, fiscal years 2002-2006, 32
- new space for Eleventh Circuit staff, 32

Miscellaneous fee schedules (*see* fees)

Morgan, Virginia M., 4

Office of Management and Budget, 32

Omnibus Crime Control and Safe Streets Act of 1968, 6

PACER (*see* Public Access to Court Electronic Records)

Panel attorneys (*see* Criminal Justice Act; defender services)

Personnel, court

- bonuses for automation, 26
- disabled, reasonable accommodations, 18-19, 25-26
- ergonomics, 33
- law clerk student loan deferrals, 26-27
- personal assistants for disabled, 18-19, 25-26
- professional liability insurance, 19, 26
- recruitment and retention bonuses, 26

Pilot programs

- recruitment and retention bonuses, 26

Place of holding bankruptcy court, 9

President of the United States, 24, 32

Pretrial services system (*see* probation and pretrial services system)

Probation and pretrial services officers (*see also* personnel, court; probation and pretrial services system)

personal assistants for disabled, 25-26

professional liability insurance, 26

risk prediction index, 17

Probation and pretrial services system

professional liability insurance, 26

risk prediction index, 17

Professional liability insurance, 19, 26

Public Access to Court Electronic Records (PACER) (*see also* fees)

Service Center search fee, 13

Records, location, 7-8

Regulations of the Judicial Conference of the United States for the Selection, Appointment, and Reappointment of United States Bankruptcy Judges, 8

Resident alien proviso, 21-22

Resolution

Rogers, Harold, 6

Retirement

bankruptcy judges, 10

Civil Service Retirement System, 10

funds, judiciary contribution, 10

magistrate judges, 10

Risk prediction index, 17

Rogers, Harold, 6

Rule of law programs, 23

Rules of practice and procedure, 31

Civil Rule 5(d), 16

copies of local rules, 14

Rules of Practice and Procedure, Committee on, 31

Salaries (*see* compensation)

Security

court security officers

medical standards, 34

physical examinations, 34

information technology, 6

Security and Facilities, Committee on, 4, 16, 32-34

Small, A. Thomas, 4

Social security appeals, 15-16

Space and facilities

construction submission process, 32

courthouse construction funding, 32

courtroom sharing, 16, 33-34

ergonomics in the workplace, 33

Five-Year Courthouse Project Plan, 32

jury boxes in bankruptcy courtrooms, 33

release of non-resident court facilities, 32

space for Eleventh Circuit staff, 32

U. S. Courts Design Guide, 33

Staff attorneys

code of conduct, 10-12

conflict of interest, 10-12

Supporting personnel (*see* personnel, court)

Technology (*see* information technology)

Temporary Emergency Fund (TEF), 27

March 14, 2001

Travel, judges'

alternative subsistence rate, 5

United States Marshals Service, 34

United States Sentencing Commission, 7, 17

U. S. Courts Design Guide, 33

Wiretap reports, 6



ADMINISTRATIVE OFFICE OF THE U.S. COURTS
THURGOOD MARSHALL FEDERAL JUDICIARY BUILDING
WASHINGTON, D.C. 20544



THE THOMAS W. WATHEN ACADEMY OF INDUSTRIAL SECURITY

THE NATIONAL INTELLECTUAL PROPERTY LAW INSTITUTE

TRADE SECRET PROTECTION AND ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

Chaired by: Peter J. Toren, Partner, Brown & Wood LLP



Wednesday, March 28, 2001

- | | |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8:00 am | REGISTRATION AND COFFEE |
| 8:30 am | Welcome and Opening Remarks
<i>Professor James P. Chandler, National Intellectual Property Law
Institute (NIPLI), Peter J. Toren, Brown & Wood, LLP</i> |
| 8:45 am | Electronic Information and Challenges of Secrecy
<i>Maynard C. Anderson, Arcadia Group Worldwide,
Former Acting Deputy Under Secretary for Security Policy
U.S. Department of Defense</i> |
| 9:45 am | BREAK |
| 10:00 am | Prosecution and Government Perspectives
<i>David Green, Deputy Chief, Computer Crime and Intellectual
Property Section, U.S. Department of Justice
Lead Prosecutor, United States v. Four Pillars, et al.
Joseph Metcalfe, Trial Attorney, Computer Crime and Intellectual
Property Section, U.S. Department of Justice</i> |
| 11:00 am | Conducting Corporate Investigations of Theft of Trade Secrets
<i>Lynn E. Mattice, Director of Corporate Security, Boston Scientific
Corporation</i> |

12:00 pm	LUNCH
1:30 pm	Conducting Competitive Intelligence Investigations <i>William DeGenaro, DeGenaro & Associates</i>
2:15 pm	The Impact of the EEA on Competitive Intelligence Investigations <i>Richard Horowitz, Attorney and SCIP Member</i>
3:00 pm	BREAK
3:15 pm	Protecting Confidential Corporate Information <i>Peter J. Toren, Moderator</i>
4:15 pm	Wrap Up
6:00 pm	Cocktails and Gala Dinner / Dance Honoree: Thomas W. Wathen <i>The Four Seasons Hotel, Washington, D.C.</i>

Thursday, March 29, 2001

8:00 am	COFFEE AND INTRODUCTIONS
8:30 am	Working With the Government: The Pros and Cons of Making a Criminal Case <i>Peter J. Toren, Brown & Wood, LLP</i>
9:30 am	BREAK
9:45 am	Trade Secret Law in the Federal Courts <i>Evan A. Raynes, Attorney, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP</i>
10:45 am	Proposed New Federal Trade Secret Law Amending the EEA and Creating Civil Remedies <i>Professor James P. Chandler, NIPLI</i>
11:30 am	Panel <i>Moderator: Peter J. Toren</i> <i>Panelists: Joseph Metcalfe, Richard Horowitz, Evan Raynes, Lynn Mattice, William DeGenaro and David Green</i>
12:00 pm	Concluding Remarks and Adjournment <i>Peter J. Toren, Professor James P. Chandler</i>

Biographical Information for Joseph Metcalfe

Joseph Metcalfe is a Department of Justice trial attorney in the Computer Crime and Intellectual Property Section in the Criminal Division. In this capacity, Mr. Metcalfe deals with a wide variety of legal issues that arise in relation to new technologies. Mr. Metcalfe has participated in investigating and prosecuting cases involving computer intrusions, criminal copyright and trademark crimes, and the seizure of electronic information. The primary focus of Mr. Metcalfe's work in the Computer Crime Section relates to enforcement of the Economic Espionage Act.

Since 1995, Mr. Metcalfe has been an Adjunct Professor of Law at Georgetown University Law Center. Prior to working at the Justice Department, he served as staff attorney with the Public Defender Service for the District of Columbia for six years. He began his legal career as an E. Barrett Prettyman Fellow in the Criminal Justice Clinic at Georgetown University Law Center.

Mr. Metcalfe received his J.D. from Harvard Law School and a Bachelor of Arts from Stanford University.

Contact Information:
Department of Justice
Computer Crime and Intellectual Property Section
1301 New York Avenue, N.W., Suite 600
Washington D.C. 20530
Phone – 202-514-1026
Fax: – 202-514-6113

LYNN E. MATTICE

Mr. Mattice is Corporate Director of Security for Boston Scientific Corporation headquartered in Natick, Massachusetts. Boston Scientific is one of the world's largest medical device company, specializing in state-of-the-art minimally invasive medical and surgical products. In addition, he heads his own consulting firm specializing in innovative security, loss prevention and risk management programs. His key areas of focus include: intellectual property & information security, due diligence, vulnerability analysis, strategic planning, crisis management and contingency planning, as well as process management methodology and effective use of business measurements in security. His peers have recognized him as a visionary for his utilization of total quality/continuous improvement techniques in the development of global security and loss prevention programs that create shareholder value and produce measurable results. Mr. Mattice has served as Corporate Security Director for three major corporations. His experience base traverses the defense, intelligence, electronics, medical, consumer products and service industries. Additionally, he headed a university affiliated educational institution dedicated to serving the law enforcement and private security sectors.

He is a past Chairman of the Board of Directors for the National Intellectual Property Law Institute in Washington, D.C. and remains a counselor to the President of the Institute. Mr. Mattice is also an industry advisor to the National Counterintelligence Center and served as a member of the U.S. State Department's Overseas Security Advisory Council. He was one of eleven industry representatives appointed to a joint government and industry task force established by Presidential Directive in 1991, focused at developing a new National Industrial Security Program (NISP) to replace the myriad of duplicative government security regulations. Mr. Mattice was recognized for his efforts as one of the principal architects of the NISP by way of a special joint commendation signed by the Secretary of Defense, Director of Central Intelligence and the Secretary of Energy. In 1992, he received a special commendation from the Department of Defense citing his visionary leadership in the advancement of security education. The Federal Bureau of Investigation honored him in 1996 with its *Outstanding Community Service Award for Law Enforcement Assistance*, along with a personal letter of commendation from Director Freeh.

Mr. Mattice was approached by the President of the American Society for Industrial Security in late 1992 and was asked to lead a special ad hoc group charged with determining the best manner in which to institute total quality management and other business-based processes in the security profession. Subsequently ASIS created a Council on Business Practices and appointed Mr. Mattice as the Charter Chairman of the Council. He has served on the Strategic Visioning Committee, Membership Committee and Education Committee for the International Security Management Association. He was instrumental in establishing an Executive Development Education Program Series for the membership of the International

Security Management Association in 1999 and he currently chairs the committee responsible for those programs.

He is a frequent guest lecturer on a variety of business and security related topics such as: *Total Quality Management for Security; Understanding Intellectual Capital and How To Protect It; Strategic Planning for Security Professionals; Developing Effective Business Enterprise Safeguards; Corporate Security - As A Value Creating Business Unit.*

Mr. Mattice attended school at California State University - Long Beach and served on the Advisory Board for the Graduate and Undergraduate level Leadership and Management Program in Security (LaMPS) at Michigan State University in East Lansing, Michigan. Mr. Mattice has also been certified as an Expert Witness at both the Federal and State Court level.

Professional affiliations include the International Security Management Association, the American Society for Industrial Security, American Society for Quality Control, Society for Competitive Intelligence Professionals and the International Association of Chiefs of Police.

PROFESSOR JAMES P. CHANDLER

President of the
NATIONAL INTELLECTUAL PROPERTY LAW INSTITUTE
Chairman of
THE CHANDLER LAW FIRM CHARTERED
B.A., University of California, Berkeley
J.D., University of California, Davis
LL.M., Harvard University

During his illustrious career, Professor James P. Chandler has compiled an enviable academic record while distinguishing himself in numerous areas of both United States and international law. His professional life is notable for the continuous offering of both his time and expertise to help create and maintain organizations dedicated to the advancement of his profession.

A gifted academic, Professor Chandler received a Graduate Fellowship to Harvard University in 1970 where he was a scholar in residence and in 1971 was a Fellow in the Academy of Engineering of the National Academy of Sciences. In 1972, Professor Chandler accepted an appointment as a Faculty Fellow in the Stanford University Engineering Department followed by an appointment in 1975 as Distinguished Visiting Professor of Law at the University of Mississippi School of Law. Breaking new ground, Professor Chandler moved to Washington, D.C. in 1977 to accept an appointment as Professor of Law and Director of the Computers in Law Institute at the George Washington University National Law Center. Professor Chandler's reputation as a pioneer and leading expert in the field of intellectual property law grew rapidly and in 1984 he returned to his *alma mater*, Harvard University, as a Visiting Scholar. Since taking Emeritus status from the George Washington University in 1994, he has been pursuing the advancement of the study and practice of intellectual property law in the United States and around the world.

The Science and Technology Section of the American Bar Association owes its founding, in part, to Professor Chandler. He served as a member of the Section Council and as academic advisor to the Section, which addresses legal problems and complications arising from the creation of new technologies. In another capacity for the Bar Association, Professor Chandler served as vice-chairman of the International Intellectual Property Rights Committee and as a member of the National Security Advisory Committee.

Recognizing the need for legal guidance in the area of computer law, Professor Chandler lent his expertise to help create the Computer Law Association of America. This Association, which specializes in the law governing computing technologies, included him on its Board of Directors from 1972 to 1982.

Professor Chandler has spent much of his professional life in the classroom all around the United States and around the world. He receives numerous invitations to lecture internationally and has been active in the international legal community since 1975. In recent years, he has

lectured at the Russian Intellectual Property Law Institute in Moscow, Kyoto University in Japan, Sun Yat Sen University and the Schiead Patent Agency in Guangzhou, China, Beijing University, Shanghai University, and Ankara University in Turkey. His advice and counsel is sought regularly from intellectual property lawyers and professionals, judges, and government representatives from all over the world, including Africa, Asia, the Middle East, Europe and the Americas. He receives students from the United States and around the world to participate in lectures, symposia, courses and seminars in Washington, D.C. where he offers advanced intellectual property law training and scholarship as President of the NATIONAL INTELLECTUAL PROPERTY LAW INSTITUTE (NIPLI).

In addition to his professorships and academic affiliations, Professor Chandler has numerous publications to his credit as well as being the co-author of a teaching text on computer law and author of a treatise on patent law. He recently published an article on Patent Protection of Computer Programs in the *Minnesota Intellectual Property Review*. Professor Chandler is the original author of the *Economic Espionage Act of 1996* (EEA) and worked closely with the Executive and Legislative Branches of the U.S. Government in support of the enactment of this legislation. He is frequently consulted by the U.S. Government, legal community, and private industry in the fields of economic espionage, intellectual property, and information and systems security issues arising from the use of computer technologies. So prominent is his reputation in the field of intellectual property law that from 1993 to 1995 Barclays Law Publishers published his analyses of cases decided by the United States Court of Appeals for the Federal Circuit.

At the request of President Clinton, Professor Chandler recently accepted an appointment to the National Infrastructure Assurance Council (NIAC), a council established by Executive Order in July 1999. The NIAC's mission is to enhance the partnership of the public and private sectors to address threats to the Nation's critical infrastructure. It will provide recommendations born of its work to both the National Security Council and the National Economic Council.

Professor Chandler is truly a leading figure and admirable scholar in intellectual property law and in the protection of United States national and economic security. His career has been both lengthy and fruitful. His former and present contributions to academia, government and the private sector will be long remembered and revered.

Peter J. Toren

Mr. Toren is a partner with Brown & Wood LLP in New York City, where he is the co-head of the Intellectual Property Group. He specializes in patent, copyright, trademark, trade secret and cyberlaw litigation. He is also an Adjunct Professor of Law at Hofstra University Law School where he teaches cyberlaw. Before entering private practice, Mr. Toren was one of the first trial attorneys with the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice. While at Justice, he was in charge of prosecutions for violations of copyright, trademark and trade secret law and the Computer Fraud and Abuse Act.

He is the author of numerous articles on a variety of Intellectual Property and cyberlaw related topics, including *Software and Business Methods are Patentable in the U.S. (Get Over It); Patent Problems? The Solution . . .*; *Protecting Inventions as Trade Secrets: A Better Way When Patents are Inappropriate, Unavailable*; *Protecting Prevailing Intellectual Property*; *Intellectual Property Due Diligence in the Acquisition of or Investment in Technology Companies*; *The Patentability of Business Methods*; *The Criminalization of Trademark Counterfeiting*; *EEA Violations Could Trigger Criminal Sanctions*; *Federal Prosecution of Violations of Intellectual Property Rights (Copyrights, Trademarks and Trade Secrets)*; and *Understanding the Economic Espionage Act of 1996*.

He is also a columnist and member of the advisory board of E-Commerce Law Journal and is writing a book on intellectual property crimes. Finally, he has lectured extensively on protecting intellectual property rights and on cyberlaw issues and has taught U.S. law to Russian judges, prosecutors and defense attorneys through the Central and East European Law Initiative ("CEELI") sponsored by the American Bar Association.

In addition to a law degree, Mr. Toren has a masters degree in International Affairs from Columbia University.

MAYNARD C. ANDERSON

Currently, President and Managing Director of Arcadia Group Worldwide, Inc., engaged in matters of national and international security. He is founder of the nonprofit *Arcadia Institute*, and a principal in the Strategic Trade Advisory Group, Inc. He has served as a Member of the Board of Directors and Faculty in the field of counterintelligence in the **National Intellectual Property Law Institute** since 1993.

Until February 1994, Mr. Anderson was the acting *Deputy Under Secretary of Defense for Security Policy*, with permanent assignment as the *Assistant Deputy Under Secretary of Defense for Security Policy*. He was responsible for providing staff advice and assistance to the Under Secretary of Defense for Policy and the Secretary of Defense in the development of overall defense policy for international security programs, national disclosure policy, special access programs, NATO security, the Foreign Disclosure and Technical Information System (FORDTIS), and related security policy automation systems, as well as emergency planning and preparedness, crisis management, and special and sensitive activities. He chaired the National Foreign Disclosure Policy Committee which determines what classified weapon systems the United States will share with foreign countries.

Formerly, Mr. Anderson served as the *Assistant Deputy Under Secretary of Defense (Counterintelligence and Security)*, from 1988-1991, with responsibilities for the management of DoD investigative, security and counterintelligence programs. He served as the focal point for counterintelligence and security policy matters within the Department of Defense and provided day-to-day oversight of world-wide DoD counterintelligence activities. In addition, he served as Chairman of the Advisory Committee for the DoD Security Institute, the DoD Polygraph Institute, and the Defense Personnel Security Research and Education Center. He also chaired the National Advisory Group/Security Countermeasures.

As Director for Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy, 1982-1988, he had responsibilities for reviewing and formulating policies that govern the security practices and programs of the Department of Defense. He also served as the *United States Representative to the NATO Security Committee*; Member, Director of Central Intelligence Security Forum; Chairman, National Industrial Security Advisory Committee; Chairman, Physical Security Review Board, Department of Defense; and Chairman, US/Canada Security Committee. In the office of the Secretary of Defense, he also served as the Deputy Director for Security Policy from 1978-1982.

Mr. Anderson was the *Director, Special Security and Special Activities, Department of the Navy*, 1973-1978; *Assistant Head, Internal Security Division, Naval Investigative Service Headquarters*, 1969-1973; *Supervising Agent, Naval Investigative Service Office, Guantanamo Bay, Cuba*, 1968-1969, Member of the Special Operations Group; Headquarters, 1966-1968; and Senior Resident Agent, Saigon, 1964-1965.

Mr. Anderson received the Presidential Rank Award of Meritorious Executive in 1985 and 1992. In 1989, he received the Distinguished Service Award from Luther College. He was the 1990

recipient of the National Classification Management Society's Donald B. Woodbridge Award of Excellence. In 1992, he received the Department of Defense Distinguished Civilian Service Award for exceptional contributions to the national security.

Mr. Anderson was born in 1932 in Iowa, is a graduate of Luther College and the Federal Executive Institute. His military service was with the United States Army Counterintelligence Corps as a special agent.

Mr. Anderson has lectured and written extensively on various aspects of management, policy, strategic planning, counterintelligence, security concepts, philosophies and disciplines, as well as national security issues. He is an honorary faculty member of the Defense Security Institute. He has been a lecturer in the School of Criminal justice, College of Social Science, Michigan State university, and is an advisor to the Leadership and Management Program in Security. He lectures at Luther College in the Department of Political Science.

In 1996, he was a lecturer and seminar leader at the Nobel Peace Prize Forum; a participant and lecturer at Vision 2021, a conference concerning security in the 21st century; and an advisor to the Commission on Protecting and Reducing Government Secrecy chaired by Senator Daniel Patrick Moynihan.

Mr. Anderson is Chairman Emeritus of the Board of Directors of the National Intellectual Property Law Institute. He is a past Director of the Security Affairs Support Association (SASA) and continues to serve as the Chairman of the SASA Policy Committee. He is serving in a four-year appointment as an industry member of the National Industrial Security Program Policy Advisory Committee. Mr. Anderson is a member of the President's Council, the Philanthropic Honor Society of Luther College, and a Biographee in *Who's Who in America (50th Edition)*.



Index

[Home](#)

[Services](#)

[Start-ups](#)

[Counter-
Intelligence](#)

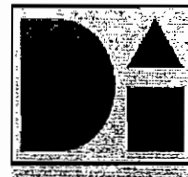
[Trade Show
Intelligence](#)

[CEO/COO
Questionnaire](#)

[Experience](#)

[Contact Us](#)

intelligence



**DeGenaro &
Associates,
Incorporated**

Business Intelligence Services

about DeGenaro & Associates...

William (Bill) DeGenaro has more than 30 years of strategic planning, intelligence and business management experience. An internationally recognized expert, he and his team have produced successful results for companies internationally.

A brief summary of Mr. DeGenaro's experience...

- ✓ President of DeGenaro & Associates
- ✓ Co-founder and principle of The Centre for Operational Business Intelligence
- ✓ Managing Director of an international consulting firm in strategic planning and business intelligence
- ✓ Director of Strategic Countermeasures Planning, Office of the Secretary of Defense for Counterintelligence and Security under the aegis of the Presidents Executive Exchange
- ✓ Director of Business Research and Analysis (Intelligence), 3M Company
- ✓ Director of Innovations Resources, 3M Company
- ✓ Strategic Planning Director, 3M Company
- ✓ Florida Private Investigators License (Florida Agency License A2000017).

Mr. DeGenaro holds a management degree from the University of Illinois at Chicago and advanced studies at the Joint Military Intelligence College in Washington DC, Harvard University, Columbia University, and University of Minnesota. He is an active member of professional organizations including Operations Security Professionals Society, Security Affairs Support Association, Strategic Leadership Forum, National Military Intelligence Officers

Association and the Association of Former Intelligence Officers. He has been elected to the board of directors of Society of Competitive Intelligence Professionals (SCIP) and is a Fellow of the Society.

DeGenaro & Associates, Inc.
1133 4th Street, Suite 200
Sarasota, FL 34236
Tel: (941) 906-9244
<http://biz-intel.com>
info@biz-intel.com

Richard Horowitz, Attorney at Law
420 Madison Avenue, Suite 300, New York, NY 10017
Tel: (212) 829-8196; Fax: (212) 829-8199; RHESQ@Compuserve.com

BIOGRAPHY

Richard Horowitz is an attorney concentrating in corporate, international, and security related issues, and holds a private investigator's license. He is a frequent speaker on issues of security and terrorism, legal issues such as money laundering, trade secret law, and the Economic Espionage Act, and on investigative and security techniques. He has spoken to companies such as AT&T-Lucent Technologies and IBM, and to numerous organizations including the American Bar Association, the American Corporate Counsel Association, the American Society for Industrial Security, the National Security Institute, and the World Association of Detectives. He has spoken at conferences in England, Belgium, Canada, Mexico, Argentina, Uruguay, Poland, and Latvia.

In addition, he has written for such publications as *Security Management*, *Money Laundering Alert*, *International Journal of Intelligence and Counterintelligence*, and the *Journal of Counterterrorism and Security International*, and has authored a Policy Analysis on Competitive Intelligence and the Economic Espionage Act for the Society of Competitive Intelligence Professionals, where he serves as a Legal Advisor.

Mr. Horowitz is a member of the Trade Secrets Committee of the American Bar Association and the Economic Crime Committee of the American Society for Industrial Security, and has served as advisor to the National Cargo Security Council on cargo and international trade related money laundering issues. He served as the security consultant for a public relations event held for Bosnia under the auspices of the President of the United Nations General Assembly, and has prepared educational material for use by the U.S. Department of Defense.

After receiving an M.A. in International Relations from New York University in 1982, he moved to Israel where he served in the Israel Defense Forces for six years, attaining the rank of captain. Upon returning to the United States, he held a Mortimer Zuckerman Fellowship from Columbia University.

January 2001

Evan A. Raynes

Evan Raynes has undergraduate and graduate degrees in history from the University of Michigan. Evan worked in the Soviet studies field for several years at the Smithsonian Institution and other think tanks. His second career in the law has focused on trademark and, more recently, trade secret issues. Evan graduated from George Washington University's law school in 1993, and currently works for Finnegan Henderson



Department of Justice

FOR IMMEDIATE RELEASE
FRIDAY, JANUARY 5, 2001
WWW.USDOJ.GOV

CRM
(202) 514-2008
TDD (202) 514-1888

JUSTICE DEPARTMENT RELEASES MANUAL TO ADDRESS INTELLECTUAL PROPERTY CRIME

Outgrowth of Intellectual Property Rights Initiative Provides Resource to Enforce Laws Against Intellectual Property Theft

WASHINGTON, D.C. - In an effort to assist law enforcement agencies across the country in combatting trademark counterfeiting, copyright piracy, and theft of trade secrets, the Department of Justice today released a manual devoted exclusively to prosecuting intellectual property crime.

The resource, entitled "Prosecuting Intellectual Property Crime," was created by the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and published by the Office of Legal Education. It contains a variety of materials including: a quick reference chart for typical IP cases; a list of commonly charged IP crimes; explanations of the criminal laws of trademark counterfeiting, copyright piracy, and trade secrets; information about recently enacted criminal IP laws such as the No Electronic Theft (NET) Act and the Digital Millennium Copyright Act (DMCA); practical advice on charging IP crimes; and contact information for relevant IP organizations and information.

"This manual will be an essential resource to federal and state law enforcement in the fight against IP crime, particularly in high-technology and cutting edge cases," said Deputy Attorney General Eric H. Holder, Jr. "At the same time that our information economy is soaring, so is intellectual property theft. With this new manual and the other efforts we have made, we are better equipped to prosecute those who steal our intellectual property."

The new manual is part of the Intellectual Property Initiative, which was launched in San Jose, California, in July 1999 by the Justice Department, the Federal Bureau of Investigation and the U.S. Customs Service. The initiative is aimed at combating the growing wave of piracy and counterfeiting offenses, both domestically and internationally, with the participation of U.S. Attorney's offices in New York, New Jersey, California, Florida and Massachusetts. The initiative has focused on training activities, improved coordination among law enforcement agencies, increased cooperation with

industry, and highlighting IP internationally. In addition, following the first-ever meeting of law enforcement experts from G-8 countries to discuss trends in trafficking in counterfeiting and pirated merchandise, hosted by the United States in September, 2000, G-8 countries agreed to address trends in trans border IP crime.

“The Department of Justice is dedicated to fighting intellectual property crime,” said Martha Stansell-Gamm, Chief of the Computer Crime and Intellectual Property Section. “The insights and practical guidance in this new manual will help us tackle the complex issues in IP cases that we are seeing every day.”

The manual will be distributed to law enforcement and industry representatives and is available to the public at www.cybercrime.gov/ipmanual.htm.

###

01-006

Competitive Intelligence and the Economic Espionage Act

**A Policy Analysis Adopted
by the
SCIP Board of Directors**



**Society of Competitive Intelligence Professionals
1700 Diagonal Road, Suite 600
Alexandria, VA 22314 USA
www.scip.org**

Copyright © 1999 by SCIP

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Introduction

In October 1996, the U.S. president signed into law the Economic Espionage Act (EEA). The EEA makes stealing or obtaining trade secrets by fraud (and buying or receiving secrets so obtained) a U.S. federal crime. Upon passage of the EEA, some members of the competitive intelligence (CI) community expressed concern that the EEA could have implications for the conduct of CI.

After the passage of the EEA, SCIP organized two symposia, one in February 1997 and another in February 1998, on the topic of CI, ethics, and law. The purpose of these events, and of several publications and articles published by SCIP, was to promote education and understanding of the law and its implications for the CI profession among SCIP's membership and in industry at large.

Many members of the Society felt it was important to develop a clear statement to define the impact of the EEA on the CI profession and clear up any confusion about the relationship between the EEA and CI. This policy statement, the result of extensive research and consultation, addresses that relationship. The policy statement was prepared by Richard Horowitz, a SCIP member who is an attorney and private investigator. It was subsequently adopted by the SCIP board of directors and endorsed by leading legal experts. Their endorsements are also included in this booklet.

Competitive intelligence is the legal and ethical collection and synthesis of data and information to enhance business decision making. SCIP members endorse this definition.

— Ava Harth Youngblood, SCIP '98-99 president

SCIP Code of Ethics for CI Professionals

- To continually strive to increase respect and recognition for the profession.
- To pursue one's duties with zeal and diligence while maintaining the highest degree of professionalism and avoiding all unethical practices.
- To faithfully adhere to and abide by one's company's policies, objectives and guidelines.
- To comply with all applicable laws.
- To accurately disclose all relevant information, including one's identity and organization, prior to all interviews.
- To fully respect all requests for confidentiality of information.
- To promote and encourage full compliance with these ethical standards within one's company, with third party contractors, and within the entire profession.

Introduction to the SCIP Policy Analysis on Competitive Intelligence and the Economic Espionage Act

Richard Horowitz, Esq.
Legal and Investigative Services
400 Madison Avenue, Suite 1411
New York, NY 10017, USA
Tel.: +1.212.829.8196
Fax: +1.212.829.8199
RHESQ@compuserve.com

Under the auspices of the SCIP ethics committee and as requested by the SCIP board of directors, I have prepared this policy analysis, adopted by SCIP's board of directors.

The question of the EEA's effect on CI has been an issue of concern in the CI industry. I believe that the significant difficulty for many in understanding what effect if any the EEA has on CI is that this issue reflects a confluence of law and security, two topics that are not generally included in a college or graduate school education. For example, the EEA is a statute, and a statute is not prose. Statutes are written without incorporating the underlying legal principles into their wording. The frustration many have felt after reading the EEA and still not understanding how it affects CI is because these underlying legal principles which are essential to understanding the law's application will not emerge from the text, regardless of fonts, graphics, or the statute's layout on the page.

I have always maintained that CI practitioners who act consistently with SCIP's code of ethics should not run afoul of the EEA. It is my hope that this policy analysis will assist members of the CI industry to understand why this is so. For those who would like a more in-depth analysis, see my article "The Economic Espionage Act: The Rules Have Not Changed" in the July-September 1998 volume of *Competitive Intelligence Review*.

I would like to thank Elkan Abramowitz, Mark Halligan, Peter Toren and the board of directors and staff of SCIP for their assistance in the preparation of this document. A special thanks to Mark, Peter and Hamilton Loeb for their assistance to me since I took an active role in this issue. In case there are any further questions, I can be reached at the address above.

Richard Horowitz

POLICY ANALYSIS ***Competitive Intelligence and the Economic Espionage Act***

Prepared by Richard Horowitz, Esq.

For the board of directors of Society of Competitive
Intelligence Professionals

Executive Summary

Seeking competitive information in a legal and ethical manner is an integral component of healthy competition.

The EEA was enacted in order to enable federal law enforcement to investigate and prosecute acts of economic espionage. It adds federal criminal penalties to activities which were already illegal under state law. The EEA does not interfere with the way corporations are entitled to gain a competitive advantage in the marketplace by seeking information on a competitor in a legal manner.

That the EEA does not materially affect competitive intelligence (CI) does not mean that CI professionals need not be concerned about trade secret law. On the contrary, the EEA has drawn attention to the necessity of insuring that CI activities are within the parameters of trade secret law.

An understanding of trade secret law and the EEA indicates that CI professionals who have been and will continue to conduct their business in an ethical manner and consistent with established trade secret law need not be concerned about the EEA debate.

Companies that have curtailed their CI efforts out of a misplaced fear of the EEA have awarded a competitive advantage to companies whose CI activities continue unimpeded.

Background

The Society of Competitive Intelligence Professionals (SCIP) is the global professional society for practitioners of business or competitive intelligence (CI). Established in 1986, SCIP today has more than 5,000 members and continues to grow substantially year after year.

Seeking information on a competitor is an important component of healthy competition; CI is the term which has developed to describe this profession. Many corporations and executives perform this function without any formal ties to the CI profession, while others employ CI professionals or outside CI firms and practitioners. Many large corporations have established entire CI departments. Competitive intelligence is a recognized,

accepted, and legal way for businesses to gain a competitive advantage in the marketplace. This in turn accelerates the benefits to society of competition in the marketplace.

SCIP encourages its members to abide by its code of ethics; one clause in the code instructs its members to "accurately disclose all relevant information, including one's identity and organization, prior to all interviews."

The Economic Espionage Act of October 1996 (EEA) was enacted by the U.S. Congress in response to attempts by foreign entities to steal American trade secrets. It was not enacted in order to regulate the CI industry nor was it enacted in response to any problems arising out of the activities of CI professionals. Its passage however has led to various and sometimes conflicting opinions regarding the EEA and has created confusion regarding its implications for the practice of CI.

The EEA is a federal criminal law and was passed in order to enable federal authorities to investigate and prosecute acts of economic espionage.

Federal authorities charged with the responsibility of protecting national security and the national economy were confronted with the reality that laws dealing with the theft of trade secrets were state law, and needed a federal law to give them the authority to investigate and prosecute the increasing number of cases of economic espionage conducted by foreign entities. The EEA was passed to do just that.

Congress decided however that the scope of the EEA would include the theft of a trade secret by anyone, for anyone. In other words, the EEA is not limited to theft of a trade secret for a foreign entity, but encompasses theft of a trade secret by and for a domestic competitor.

Herein lies the confusion. While the EEA makes trade secret law a federal criminal matter — this for the first time in U.S. history — the activities it criminalizes had always been prohibited under state law and/or inconsistent with SCIP's code of ethics. In other words, the rules are fundamentally the same but the consequences of violating them are different. An activity that had always been a violation of state trade secret law can now result in not only state civil liability but federal criminal liability as well.

Implications

There are several reasons why the EEA should not have any impact on the practice of competitive intelligence.

First, the act of seeking and collecting information on a competitor is itself legal. Note the following from the Restatement of Torts (1939):

The privilege to compete with others includes a privilege to adopt their business methods, ideas,

or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition (Section 757, Comment a).

One limitation on this rule cited by the Restatement is: "It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of liability in this section."

Information collection performed by CI professionals centers around the sophisticated use of published material, databases, and on-the-record interviews, techniques which themselves are legal and proper means of acquiring information.

Second, properly trained CI professionals who have conducted themselves in an ethical manner were not engaged in legally risky business prior to the EEA. The appropriate legal principles have been instilled into the CI profession over the years of its existence and subsequently adopted as practice by properly trained industry members. The increased penalties for trade secret theft under the EEA will not be applicable to those whose practice has been consistent with the already existing legal standards.

Third, most situations commonly referred to as "gray zone" areas are not trade secret violations at all. Though they raise ethical questions, "gray zone" situations such as finding a lost document in the street, overhearing competitors talk on a plane, having a drink with a competitor knowing you are better at holding your liquor, removing your name tag at a trade show, or even falsely identifying yourself as a student, are situations which alone will not trigger trade secret liability. Properly trained CI professionals should be able to identify and avoid the predicaments that would place them in actual legal risk.

Fourth, the EEA will not be applied to general commercial disputes, but to clear criminal acts of theft. The reason for the EEA's passage was to thwart attempts at stealing American trade secrets which would have an impact on the competitiveness and health of the American economy. That the U.S. Attorney General promised Congress that no charges will be filed under the EEA for the first five years after the law's enactment without the approval of the Attorney General or two of her top deputies indicates that federal authorities have no intention of becoming entangled in the numerous trade secret disputes that do take place in the routine course of business (see Congressional Record, October 2, 1994, S12214).

To summarize, the EEA incorporates into the federal criminal code activities that were already illegal under state law. It does not add new burdens or restrictions to the American workforce.

A Note on Extraterritoriality

About twenty percent of SCIP's membership is outside the USA, making the question of how the EEA affects overseas activity pertinent.

The EEA does have an extraterritoriality clause. In principle, a statute must state that it applies overseas for it to so apply. The extraterritoriality provisions of the EEA apply the statute to a U.S. citizen even abroad, and to a non-U.S. citizen (1) while on U.S. soil or (2) abroad, if the act committed abroad violates the EEA and "an act in furtherance of the offense was committed in the United States."

What this means in practice is that whatever types of activities the EEA prohibits overseas are the same as what is prohibited on U.S. soil, which, as explained, had always been prohibited by state law and/or inconsistent with SCIP's code of ethics.

EEA Compliance Plans

An additional reason for concern regarding the implications of the EEA on competitive intelligence has been the many calls for "EEA compliance plans" based on the Federal Sentencing Guidelines. The Sentencing Guidelines do not instruct, dictate, require, prescribe, or obligate a company to have a compliance plan. The Sentencing Guidelines, the manual by which federal judges must sentence a defendant, allows the judge to deduct "points" from the sentence, i.e., lessen the sentence, if a *corporate* defendant, not an *individual* defendant, took measures to "detect and prevent" the criminal activity from occurring. A proper compliance can lower the sentence of a corporation convicted of a crime; it has no relevance to the sentencing of an individual convicted of a crime.

The list of seven "must haves" from the Sentencing Guidelines, referred to in EEA compliance plan articles and presentations are not obligatory (i.e., "The organization must have established compliance standards and procedures . . . the organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents..."). The document is talking to the judge, not the corporate defendant. The corporate defendant "must have" taken these steps in order for the judge to find that a reasonable plan to "detect and prevent" crime was in place, not that the company "must have" done these things as an independent legal obligation.

The Sentencing Guidelines do not actually use the phrase "compliance plan." This is the term which has developed to refer to the measures to "detect and prevent" violations of law. A company that does not have a compliance plan is not "in violation" of the Federal Sentencing Guidelines, and if not convicted of a particular crime, the

lack of a compliance plan for that aspect of law will be of no consequence. Conversely, a company convicted of a federal crime will not be penalized for not having a compliance plan but will lose its chance of receiving a lowered sentence. Though not a legal requirement under the Guidelines, in practice having a compliance plan is the responsible and indeed the expected way for a company to conduct its affairs.

There are no "EEA regulations" to *comply with*. One is to learn what not to do and not do it. Generally speaking, compliance plans are geared to aspects of law that are industry specific and encompass regulations. Banks will have a compliance plan for Treasury Department regulations, pharmaceutical companies for FDA regulations, securities dealers for SEC regulations, and telecommunications companies for FCC regulations. As the activities the EEA criminalizes are substantially the same activities in which CI professionals should never have been engaged, an EEA "compliance plan" should not be substantially different from the existing professional guidelines a CI firm or professional would be expected to have or abide by.

Answers to Frequently Asked Questions

1. Even if the EEA was not intended to deal with competitive intelligence or general commercial disputes, hasn't it had an impact nonetheless?

Answer: The impact the EEA has had on the CI community has been based on anxiety and confusion. Some companies have mistakenly taken the position that the EEA has placed them in legal jeopardy because of the activities of their CI professionals.

Ironically, companies who curtail the legal and ethical activities of their CI professionals have placed themselves at a competitive disadvantage to companies whose CI activities continue unimpeded.

2. Don't we have to wait to see how the EEA is applied in the courts before determining what it prohibits?

Answer: How courts ultimately interpret statutes is a fundamental part of legal analysis. This does not mean however that one cannot understand the basic prohibitions of a statute. In fact, a statute can be declared unconstitutional by the courts if it does not provide adequate notice as to what it prohibits.

The intention and purpose behind the EEA was clearly explained by Congress prior to its enactment. This did not include an intention to alter the fundamentals of corporate conduct, but to deter and punish the criminal act of trade secret theft.

3. Can't the EEA be applied to situations it was not intended to cover?

Answer: It is not unusual for some laws to ultimately be applied to unforeseen situations. A law once passed may take on a life of its own. The concern that the EEA will be applied to routine commercial disputes was discussed and dismissed by Congress prior to the EEA's passage, with the Attorney General's letter giving further assurances to this effect (see page 4). Companies who remain concerned are well-advised to study the background of the law.

4. The definition of a trade secret under the EEA is broader than existing trade secret law. What implications does this have on competitive intelligence?

Answer: The wording of the EEA's definition enumerates more types of information considered a trade secret than previous legal definitions. This is because a criminal statute should be written in explicit language so as to give notice as to what it criminalizes, otherwise it risks being declared unconstitutional. This does not mean that prior legal definitions excluded types of information enumerated in the EEA's definition.

In practice, existing legal definitions and case law interpretations cover all sorts of financial, business, and scientific information.

Whether the information stolen is included in the EEA's definition of a trade secret is moot with respect to professionals whose conduct precludes them from engaging in theft.

5. What effect if any does the EEA have on the legal risks one may decide to take in seeking information on a competitor?

Answer: The EEA compounds the legal consequences for one engaged in theft of a trade secret by adding federal criminal penalties to an act which already triggers state civil penalties. This added risk however is of no consequence to one who seeks information on a competitor in a legal manner.

6. What implication does the EEA have on a company's efforts to protect information?

Answer: The EEA focuses primarily on the activities it prohibits. The EEA's definition of a trade secret however, like state trade secret law preceding it, requires the trade secret holder to take reasonable measures to keep that information secret. In practice, the holder of a trade secret must have taken those reasonable measures in order for one who misappropriates that information to be held liable under the EEA or state trade secret law.

WELSH & KATZ, LTD.

Attorneys at Law

120 SOUTH RIVERSIDE PLAZA - 22ND FLOOR
CHICAGO, ILLINOIS 60606

TELEPHONE (312) 655-1500

FACSIMILE (312) 655-1501

A. SIDNEY KATZ*
RICHARD L. WOOD*
JEROLD B. SCHNAYER
ERIC C. COHEN
JOSEPH R. MARCUS
GERALD S. SCHUR
GERALD T. SHEKLETON
JAMES A. SCHEER
DANIEL R. CHERRY
ROBERT B. BREISBLATT
JAMES P. WHITE
R. MARK HALLIGAN
HARTWELL P. MORSE, III
EDWARD P. GAMSON, Ph.D.
KARA E.F. CENAR
KATHLEEN A. RHEINTGEN
THOMAS W. TOLPIN*
ELLIOTT C. BANKENDORF
RICHARD W. McLAREN, JR.
JOHN L. AMBROGI
JULIE A. KATZ
JON P. CHRISTENSEN

* ALSO ADMITTED IN DISTRICT OF COLUMBIA

ERIC D. COHEN
WALTER J. KAWULA, JR.
LEONARD FRIEDMAN
STEVEN E. FELDMAN
IK HYUN SEO
PHILIP D. SEGREST, JR.
JEFFREY W. SALMON
MITCHELL J. WEINSTEIN
SHANNON L. NEBOLSKY, Ph.D.
ELIZABETH D. McGOOGAN
RICHARD J. GURAK
SCOTT M. GETTLESON
J. ARON CARNAHAN
MICHAEL A. BONDI
RALPH E. KRISHER III
THOMAS L. GEMMELL
LOUISE T. WALSH

OF COUNSEL
DONALD L. WELSH
LAURIE A. HAYNIE

WASHINGTON OFFICE
CRYSTAL PLAZA ONE - SUITE 206
2001 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VIRGINIA 22202-3603
TELEPHONE (703) 415-4777

January 21, 1999

VIA OVERNIGHT COURIER

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandra, Virginia 22314

Re: *Competitive Intelligence and the Economic Espionage Act*

Dear Board Members:

As you know, I teach trade secrets law at John Marshall Law School and I am an active practitioner and retained expert in trade secret cases around the country. See <http://www.execpc.com/~mhallign/resume1.html>.

At Richard Horowitz's request, I have reviewed his (8/17/98) draft entitled "Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act."

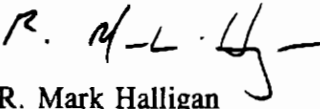
This is a well written draft and I endorse it. I strongly agree with the basic underlying premise -- The EEA does not materially affect competitive intelligence activities and companies should not curtail competitive intelligence activities based on a "misplaced fear" of the EEA. In fact, just the opposite is true. Companies should increase competitive intelligence activities to meet the challenge of an increasingly global competitive environment.

My summary of "Reported Criminal Arrests Under the Economic Espionage Act of 1996" is the most up-to-date information available on EEA prosecutions and convictions. It is available on the Internet at <http://www.execpc.com/~mhallign/indict.html>. As you can see, these EEA prosecutions involve trade secret theft and bear no reasonable relationship whatsoever

to legitimate competitive intelligence activities.

If I can be of further assistance to the SCIP Board of Directors, please contact me at 1-312-526-1559.

Very truly yours,

Handwritten signature of R. Mark Halligan in black ink, consisting of the letters 'R. M-L' followed by a stylized 'H' and a horizontal line.

R. Mark Halligan

RMH/js

cc: Richard Horowitz, Esq.

Peter J. Toren
525 University Ave.
Palo Alto, CA 94301

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, VA 22314

Re: Economic Espionage Act of 1996

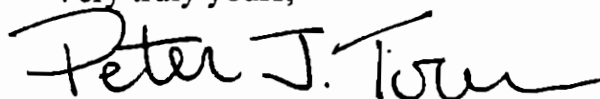
Dear Board Members:

I was formerly a trial attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice where I was involved in drafting the Economic Espionage Act of 1996 ("EEA"), and was the lead prosecutor on one of the first cases brought under the EEA. In addition, I am a co-author of an article entitled "Understanding the Economic Espionage Act of 1996," 5 Tex. Int. Prop. L.J. 177 (Winter 1997). Currently, I am a Special Counsel in the San Francisco and Palo Alto offices of Heller Ehrman White and McAuliffe.

At Richard Horowitz's request, I have reviewed SCIP's "Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act" and offer the following comments.

The EEA was intended to address both the general need for a federal criminal deterrent against trade secret theft and the apparent threat of industrial espionage sponsored by foreign countries. The EEA was not intended to impose new restrictions on American businesses. I agree with the Policy Analysis that the EEA was not developed in order to regulate the competitive intelligence community, nor was it developed in response to any problems that might have existed in the competitive intelligence community. Competitive intelligence practitioners who abide by SCIP's Code of Ethics should not be in violation of the EEA. If I can be of further assistance to the SCIP Board of Directors, please call me at (650) 324-7156 or e-mail me at bmtsdad@AOL.com.

Very truly yours,



Peter J. Toren

MORVILLO, ABRAMOWITZ, GRAND, IASON & SILBERBERG, P.C.

ELKAN ABRAMOWITZ
ROBERT J. ANELLO
LAWRENCE S. BADER
BARRY A. BOHRER
CATHERINE M. FOTI
PAUL R. GRAND
LAWRENCE IASON
ROBERT G. MORVILLO
DIANA D. PARKER
MICHAEL C. SILBERBERG
EDWARD M. SPIRO
JOHN J. TIGUE, JR.
RICHARD D. WEINBERG

COUNSEL
ROBERT J. MCGUIRE
MICHAEL W. MITCHELL

565 FIFTH AVENUE
NEW YORK, N.Y. 10017

TELEPHONE
(212) 856-9600

CABLE: LITIGATOR, NEW YORK

FACSIMILE
(212) 856-9494

WRITER'S DIRECT DIAL
880-9500

March 2, 1999

DAVID AXINN
ANIRUDH BANSAL
NEIL M. BAROFSKY
DAVID A. BATTAT
STEVEN H. BRESLOW
MICHAEL F. BUCHANAN
JAMES C. DUGAN
REBECCA A. GLASER
R. JOSEPH GRIBKO
RACHEL M. HEALD
MICHAEL R. MARRA
MARC E. MASTERS
HELEN L. MONACO
GRETCHEN R. OHLIG
JODI MISHNER PEIKIN
MAE C. QUINN*
JOSHUA H. REISMAN
ELIZABETH SMALL
PETER M. SPETT
JOSEPH C. SPONHOLZ
ALISON VAN HORN

*ADMITTED ONLY IN DISTRICT OF COLUMBIA

BY FEDERAL EXPRESS

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, VA 22314

Re: Economic Espionage Act of 1996

Dear Board Members:

I am a former Chief of the Criminal Division of the United States Attorney's Office for the Southern District of New York and co-author of the chapter entitled "Corporate Sentencing Under the Federal Guidelines," in Obermaier and Morvillo, White Collar Crime: Business and Regulatory Offenses.

At Richard Horowitz's request, I have reviewed his (1/27/99) draft entitled "Proposed Policy Analysis: Competitive Intelligence and The Economic Espionage Act," particularly the section dealing with the sentencing guidelines and compliance plans.

Mr. Horowitz has written an interesting and informative submission, pointing out the relationship between compliance plans and the Federal Sentencing Guidelines as they relate to corporations. His analysis is incisive and important.

SCIP Board of Directors

- 2 -

March 2, 1999

I agree with his analysis that the Federal Sentencing Guidelines do not create a legal obligation for a corporation to create a compliance plan.

If I can be of further assistance to the SCIP Board of Directors, please feel free to contact me at the above number.

Very truly yours,

Elkan Abramowitz / MB

Elkan Abramowitz

EA/cs

cc: Richard Horowitz, Esq.

The Economic Espionage Act: The Rules Have Not Changed

Richard Horowitz, Esq.

Legal and Investigative Services

EXECUTIVE SUMMARY

The author argues that the Economic Espionage Act of 1996 was never intended to limit aggressive but legitimate competitive intelligence collection activities, nor even activities that fall into the "gray zone," and that CI professionals who are properly trained and abide by SCIP's Code of Ethics should not run afoul of trade secret law or the EEA. The clearly criminal activities the EEA targets have always been prohibited under state law and unacceptable under SCIP's Code of Ethics. Moreover, trade secret case law has interpreted "misrepresentation" as applying to situations which induce a breach of confidentiality. Using "pretexts" to elicit information may be unethical, but isn't illegal under most circumstances. © 1998 John Wiley & Sons, Inc.

The effect of the Economic Espionage Act (EEA) on competitive intelligence has become a matter of concern among many CI practitioners and firms since its enactment in October 1996. I took an active interest in this issue because of a comment made at SCIP's February 1997 EEA Symposium. During a break after the panel of lawyers, I heard one attendee ask his colleague if they now could be subject to an FBI arrest by attending a trade show without a company name on their name tag because the EEA prohibits misrepresentation.

I spoke the following day and stated that the EEA was not intended to regulate the CI community nor was it

developed in response to any problems arising from the CI community; that the EEA does not change the rules of game—only the consequences of violating them, and that my concern was not that the Department of Justice would misuse this law but that companies and their attorneys might attempt to use the EEA to intimidate their competitors who are attempting to collect competitive intelligence on them.

Since then I have come across numerous situations where CI professionals have been under pressure from their companies to curtail their activities, others who have had to endure the anxiety that their jobs may be

eliminated for fear of legal liability, and still others who are hesitant to proceed with their work, either because they are unsure of what the EEA means or what action others may take against them because of the EEA.

The peculiar irony of this situation is that CI practitioners who are properly trained and abide by SCIP's Code of Ethics should not run afoul of trade secret law or the EEA. This is because the appropriate legal standards have been instilled in the CI profession in the decade that SCIP has been in existence. Again, from personal experience I know many CI professionals who "are doing everything right" from a legal perspective but cannot explain why this is so in legal terms.

APPROPRIATE LEGAL STANDARDS HAVE BEEN
INSTILLED IN THE CI PROFESSION IN THE
DECADE THAT SCIP HAS BEEN IN EXISTENCE.

The key to understanding why the EEA is fundamentally irrelevant to CI that is conducted consistently with SCIP's Code of Ethics is to recognize that trade secret law is not new. For decades, one who misappropriated a competitor's trade secrets was subject to civil liability under state law and, in some states, criminal liability. Trade secret cases from the 19th century are still quoted in court today.

Being charged with the responsibility of protecting national security and the national economy, and, confronted with the reality that laws dealing with the theft of trade secrets were state law, federal authorities needed a federal statute to give them the authority to investigate and prosecute the increasing number of cases of economic espionage conducted by foreign entities.

The EEA was enacted to enable federal authorities to do just that.

Congress decided, however, that the scope of the EEA would include the theft of a trade secret by anyone, for anyone. In other words, the EEA is not limited to theft of a trade secret for a foreign entity, but encompasses theft of a trade secret by and for a domestic competitor.⁹

⁹Peter Toren, the Justice Department official most closely associated with the EEA, co-authored an article which contained the following: "Originally, the bill applied only to thefts of trade secrets that were intended to benefit a 'foreign government, foreign instrumentality, or foreign agent.' Concerns that such a law might violate a number of international trade treaties to which the United States is a signatory caused the bill to be rewritten at the last minute to include both foreign and domestic theft of trade secrets." ("EEA Violations Could Trigger Criminal Sanctions," by Hoken S. Seki and Peter J. Toren, *The National Law Journal*, August 25, 1997).

Herein lies the confusion. While the EEA makes trade secret law a federal criminal matter—this for the first time in U.S. history—the activities it criminalizes were prohibited under state law and/or unacceptable under SCIP's Code of Ethics. In other words, the rules are fundamentally the same, but the consequences of violating them are different. An activity that had always been a violation of state trade secret law can now result in not only state civil liability but federal criminal liability as well.

Adding to the confusion regarding the EEA has been a series of articles and presentations that has created the impression that the EEA fundamentally alters how CI professionals must conduct their affairs: "New Spy Law Could Cramp Economy,"¹¹ "New Spy Act To Boost White-Collar Defense Biz,"¹² "Go Directly To Jail: New Federal Law Protects Trade Secrets,"¹³ "U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance,"¹⁴ "The Economic Espionage Act: A Wake-Up Call,"¹⁵ "The Economic Espionage Act: Turning Fear Into Compliance,"¹⁶ "Economic Espionage Act: A Whole New Ball Game."¹⁷ Among the more notable assertions:

*"Your industry is crawling with criminals. And you may be one of them. So might your company . . . Cases involving a customer list used to be a concern only of private lawyers; now they can be investigated by the FBI and prosecuted by the Department of Justice. All of this came about with the enactment of the [EEA] . . . the fact of its passage will surely lead to greater interest in federal jurisdiction over civil trade secret disputes."*¹⁸

*"The risks of a federal offense are high and the consequences costly and severe."*¹⁹

*"The [EEA] makes theft of trade secrets a federal crime with stiff penalties of up to \$10 million and 15 years in prison for violations. Under current standards of business practice, a sales representative, vendor, consultant, market researcher, or curious employee could subject an organization to an FBI raid and investigation leading to federal prosecution."*²⁰

The first wave of pro-EEA material argued that there exists "a new list of activities" prohibited by the EEA that CI professionals must avoid. Unable to articulate what these activities are, the pro-EEA proponents now speak of a changed "risk management equation," that risks CI practitioners might have taken in the past have become untenable with the passage of the EEA.

An understanding of trade secret law and our legal system is necessary to recognize whether these assertions have merit.

That the legal consequences facing one who steals a trade secret are far more severe under the EEA does not mean that these consequences prior to its passage were not serious. It is inconceivable that responsible corporate counsel or outside attorneys would not dissuade their companies or clients from engaging in legally risky behavior if the potential sanctions were "only" state civil as opposed to federal criminal. Moreover, after much research including conversations with numerous CI industry veterans, pre-EEA litigation involving CI professionals who misappropriated trade secrets is apparently non-existent. As a criminal statute, EEA cases require a higher burden of proof than state trade secret cases, which in part explains why EEA charges filed to date have implicated clear-cut criminal activity.^b That "gray zone" activity that has in fact taken place among CI professionals did not generate state trade secret litigation indicates that the risks of the EEA being implicated in these situations is low indeed.

EEA CHARGES HAVE ONLY IMPLICATED CLEAR-CUT CRIMINAL ACTIVITY. THE RISKS OF THE EEA BEING IMPLICATED IN "GRAY ZONE" SITUATIONS IS LOW INDEED.

Another reason why the risk of the EEA being associated with routine commercial disputes is low can be found in the article co-authored by Mr. Toren,¹¹ where he wrote that the act of a U.S. citizen anywhere could violate the EEA: "This conceivably means that if a U.S. citizen residing abroad steals a Russian trade secret on behalf of the Chinese government, that act violates the EEA . . . Congress, however, likely did not intend to reach

^bOften in civil trade secret litigation, the issue essential to the case such as (1) Is the information in question a trade secret?, (2) Were reasonable measures used to keep the information secret?, (3) Were the means of acquiring the information improper?, are questions to be answered by the jury. In a criminal case, the prosecutor would want to be certain that the basic elements of the crime can be established as easily as possible rather than rely on jury deliberations. This supports the contention that EEA cases will be based on clear-cut criminal activity such as bribery and clearly recognizable trade secrets such as chemical formulas or blueprints. The five EEA cases to date support this. For a summary of these cases, see "In the Spotlight: Four Cases Under the EEA," *The Corporate Counselor*, November, 1997, and *U.S. v. Kai-Lo, U.S. v. Ho, FBI Charges Taiwanese Tried To Steal Taxol Trade Secrets from BMS*, *Intellectual Property Litigation Reporter*, June 18, 1998.

situations in which the United States does not have a legitimate national interest."

What comes to my mind is a case I learned in law school: Driver is sober, passenger drunk. Driver parks and exits the car, which begins to roll down the hill. Though drunk, passenger moves into the driver's seat, turns the steering wheel to avoid hitting a tree and applies the brakes. Police arrest passenger for being "in control of a motor vehicle" while in a state of intoxication.

Though surely beyond intention of the legislature, a strict reading of the statute would apply it to the facts of this case. Is it, however, a correct application of the law?

To insure that the EEA will not be applied to situations inconsistent with Congressional intent for the law, Attorney General Janet Reno promised Congress that no charges will be brought under the EEA for the first five years without the authorization of the Attorney General or two of her top deputies.¹²

In other words, to maintain that the EEA will be applied to commercial "gray zone" cases, one must believe, in light of General Reno's letter, that the *very top* Justice Department decision-makers would, first, take an interest in the case and, second, file a criminal charge where they could not be confident of a victory in civil court, in situations not intended to be covered by Congress.

"Gray Zone" Activities

The most significant reason, however, why the EEA should not be of concern to CI professionals who abide by the industry's standards of ethics is that many situations which have come to be known as "gray zone" activities are not really trade secret violations at all. Finding a lost document in the street, overhearing competitors talk on a plane, having a drink with a competitor knowing you are better at holding your liquor, removing your name tag at a trade show, or even falsely identifying yourself as a student, are situations that alone will not trigger trade secret liability. As I wrote in the beginning of this article, the appropriate legal principles have been instilled into the CI profession over the years and the many "gray zone" sessions sponsored by SCIP attest to this: attendees can generally (1) recognize what activities are clearly illegal, and (2) understand when to rely on their ethical instincts with respect to "gray zone" issues.

A short analysis of trade secret law as it applies to competitive intelligence is in order. Note, that the following is intended to explain the fundamentals of trade secret law and not to answer legal questions that may arise.

A paragraph from the Restatement of Torts (1939)^c which surprisingly I have not found cited in any published material on CI, points to the legal validity of competitive intelligence:

*The privilege to compete with others includes a privilege to adopt their business methods, ideas, or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition.*¹³

One limitation on this rule cited by the Restatement is:^d

when the thing copied is a trade secret . . . The significant difference of fact between trade secrets and the processes or devices which are not secret is that knowledge of the latter is available to the copier without the use of improper means to procure it, while knowledge of the former is ordinarily available to him only by the use of such means. It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of liability in this section.

Consider the following general points with respect to the applicability of trade secret law to competitive intelligence.

1. Trade secret law protects the holder of a trade secret from someone who "misappropriates" that trade secret—i.e., obtains that trade secret through "improper means."
2. Trade secret law does not protect the trade secret information itself. In other words, a trade secret is not a patent. It is legal to "figure out" another's trade secret if all the collection methods used to acquire the information were themselves legal.
3. Trade secret law considers misrepresentation an improper mean.
4. Case law has interpreted misrepresentation to apply to situations where:

- a. One has induced another to violate his duty of confidentiality to his employer.
- b. One has violated a confidential relationship with another.
- c. One has acquired a trade secret from another knowing that the other had misappropriated the trade secret or that he had violated his duty to keep the information secret.

Misrepresentation and Pretexts

How then are these principles applied to the numerous "gray zone" situations that may confront a CI professional? Has one broken the law by identifying himself to a competitor as a student?

Focusing on pretext situations, the first reason that most "gray zone" activities are not trade secret violations is because rarely does a question produce a trade secret. That a competitor would not have spoken to you had he known your real identity does not mean that what he told you was a trade secret.

THAT COMPETITORS WOULD NOT HAVE SPOKEN
TO YOU HAD THEY KNOWN YOUR REAL
IDENTITY DOES NOT MEAN THAT WHAT THEY
TOLD YOU WAS A TRADE SECRET. THAT A
COMPANY CONSIDERS CERTAIN INFORMATION
CONFIDENTIAL DOES NOT ALONE MAKE IT A
TRADE SECRET.

That a company considers certain information confidential does not alone make that information a trade secret. Most importantly, violating trade secret law requires that the misrepresentation induce a breach of confidentiality. A question that elicits an answer is not an inducement. Consider that a trade secret holder is under a duty to keep that information confidential; therefore whatever information he stated which did not encompass a violation of that duty would not be trade secret information. The competitor may very well have answered the question had the questioner truly been a student; that the questioner misrepresented himself does not mean it was the misrepresentation that induced the answer. Rather, the question itself, irrespective of the identity of the questioner, elicited an answer.

Trade secret law does not regulate the level of honesty one displays in interpersonal or even in business relations. That is the contribution of ethics. This issue of course is most provided CI professionals abide by SCIP's Code of Ethics, which expects CI professionals to accurately disclose their identity prior to all interviews. What about disclosing your identity but not your motives? One is not under a legal duty to disclose his motive or purpose.

^cA Restatement is itself not law. *Black's Law Dictionary* defines the Restatement as follows: "A series of volumes authored by the American Law Institute that tell what the law in a general area is, how it is changing, and what direction the authors (who are leading legal scholars in each field covered) think this change should take. . . The various Restatements have been a formidable force in shaping the disciplines of the law covered; they are frequently cited by courts and either followed or distinguished; they represent the fruit of the labor of the best legal minds in the diverse fields of law covered" (p. 1313, Sixth Edition, 1990).

^dThe two other limitations cited are (1) when the information is patented, and (2) "copying in a manner which creates in the market avoidable confusion of commercial source. The privilege to copy is not a privilege to palm off one's goods as those of another."

THERE IS NO LEGAL DUTY TO DISCLOSE MOTIVE
OR PURPOSE TO A COMPETITOR WHEN
ELICITING INFORMATION.

To be precise, what a trade secret means is that the law will protect that information from someone who uses improper means to acquire it. Consequently, acquiring the trade secret through legal methods does not result in a trade secret violation. Furthermore, the trade secret holder will forfeit trade secret protection if the measures taken to keep the information secret were not reasonable.

One case in point: *A* decides to sell its tangible assets but not its intellectual property. *A* sells a computer to *B* but neglects to erase its customer list from the computer's memory. After the sale, *B* visits *A*'s premises to see the computer and hires *A*'s former employee to demonstrate its use, who then prints *A*'s customer list for *B*. Did *B* misappropriate *A*'s trade secret? According to a federal court in New York, *B* did not:

*"A customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret and protected at the owner's instance against disclosure to a competitor, provided the information it contains is not readily available . . . However, the owner is entitled to such protection only as long as he maintains the list in secrecy; upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected . . . Hence even though [defendant] may have obtained the lists by improper means paying—a former employee of [plaintiff] to extract the information from the computer—any such impropriety does not create liability for use of a trade secret, since by failing to protect the lists from ready access by [defendant] independently of [the former employee's] assistance, [plaintiff] had forfeited the protections of trade secret law."*¹⁴

In the opposite extreme, there are situations where one can violate trade secret law even though the information is not technically a trade secret. This occurs when one has learned the information in the context of a confidential relationship which he then violated.

Consider the following case: *A* approaches *B* expressing his interest to sell *B*'s product. *A* falsely claims a sales force of thirteen and *B* shows *A* details about his business and product. *A* later informs *B* he would not sell *B*'s product and uses the knowledge he acquired from *B* to produce and market a similar product. *B* sues *A*, who argues that the information provided by *B* was not trade secret information. The court held:

*"It is doubtful whether [A] ever in good faith intended to sell [B's] product . . . the essence of [A's] action is not infringement but breach of faith. It matters not that [A] could have gained their knowledge from a study of the expired patents and plaintiff's publicly marketed product. Instead they gained it from [B] via their confidential relationship, and in so doing incurred a duty not to use it to [B's] detriment. This duty they have breached."*¹⁵

Consider the following two pre-EEA trade secret cases:

1. On February 2, 1996, a Japanese business executive obtained confidential information from a computer chip manufacturer by posing as a Toshiba representative, knowing that the target company had a confidential relationship with Toshiba. The man was subsequently arrested by the FBI, pled guilty to a felony charge, sentenced to time served, and was deported.¹⁶
2. In September 1996, a private investigator approached a target company posing as a graduate student and claimed to need the company's confidential information for his research. The company provided the information after the "student" agreed to signing a non-disclosure agreement, which he violated by providing his client with the information.¹⁷

It is hard to imagine that properly trained CI professionals would not understand that the activity in these cases clearly violates trade secret law. When CI professionals recognize or have a visceral feeling that a certain type of pretext activity is illegal, it is of the sort described in the above-two examples, a misrepresentation that induces a breach of confidence. Competitive intelligence "gray zone" hypotheticals do not entail the type of improper behavior anticipated by trade secret law.

COMPETITIVE INTELLIGENCE "GRAY ZONE"
HYPOTHETICALS DO NOT ENTAIL THE TYPE OF
IMPROPER BEHAVIOR ANTICIPATED BY TRADE
SECRET LAW

Several specific issues need be addressed with respect to the EEA and CI.

- A. The argument has been made that the EEA's much broader definition of a trade secret presents new dangers to those seeking competitive intelligence.*

True, the EEA's definition is broader than previous legal definitions. That is because a criminal statute should be written in explicit language to give notice as to what it criminalizes, otherwise it risks being declared unconsti-

tutional. In practice, however, the decision as to what constitutes a trade secret is not based solely on the wording of a statute but on how courts have interpreted those words. I do not know anyone who would steal a trade secret on the calculation that pre-EEA case law and statutes in the jurisdiction in which he would be tried do not cover the subject-matter of the theft.

B. Perhaps the most blatant misrepresentation of law can be found in the article "How Safe Are Your Secrets" published in the September 8, 1997 edition of Fortune magazine

Citing several hypotheticals, one them overhearing two competitors talk loudly on an airplane, *Fortune* stated "Such shenanigans are now illegal or probably illegal, since the EEA defines theft as the knowing misappropriation of a secret without its owner's consent . . . Are we saying you're obligated, now, to protect your competitors from their own stupidity? Yes."

There is absolutely no legal basis for the proposition that one must protect a competitor from his own stupidity. If however, the EEA prohibits the taking of a trade secret without the owner's consent, does one then break the law by picking up a confidential document left by a competitor in the street?

The answer is clearly of course not. Though the ethical standard would recommend to return it, a document left on the street has lost its trade secret protection. You did not receive the owner's consent to pick it up, but then again you did not need his consent to begin with.

C. Calls for "EEA compliance plans" based on the Federal Sentencing Guidelines are misleading.

The Sentencing Guidelines do not instruct, dictate, require, prescribe, or obligate a company to have a compliance plan. The Sentencing Guidelines, the manual by which federal judges must sentence a defendant, allows the judge to deduct "points" from the sentence, i.e., lessen the sentence, if a *corporate defendant*, not an *individual defendant*, took measures to "detect and prevent" the criminal activity from occurring.⁶ A proper compliance

can lower the sentence of a *corporation* convicted of a crime; it has no relevance to the sentencing of an *individual* convicted of a crime.⁶

The Sentencing Guidelines do not actually use the "phrase compliance plan." This is the term which has developed to refer to the measures to "detect and prevent" violations of law. A company that does not have a compliance plan is not "in violation" of the Federal Sentencing Guidelines, and if not convicted of a particular crime, the lack of a compliance plan for that aspect of law will be of no consequence. Conversely, a company convicted of a federal crime will not be penalized for not having a compliance plan but will lose its chance of receiving a lowered sentence. Though not a legal requirement under the Guidelines, in practice having a compliance plan is the responsible and indeed the expected way for a company to conduct its affairs.

DOES THE EEA PROHIBIT PICKING UP A
CONFIDENTIAL DOCUMENT LEFT BY A
COMPETITOR IN THE STREET? OF COURSE NOT.

Generally speaking, compliance plans are geared to aspects of law that are industry specific and encompass regulations. Banks will have a compliance plan for Treasury Department regulations, pharmaceutical companies for FDA regulations, securities dealers for SEC regulations, and telecommunications companies for FCC regulations. There are no "EEA regulations" to *comply with*. One is to learn what not to do and not do it. As the activities the EEA criminalizes are substantially the same activities which CI professionals should never have been engaged in, an EEA "compliance plan" should not be substantially different from the existing professional guidelines a CI firm would be expected to have.

Finally, a compliance plan is not a document entitled "compliance plan" printed on company letterhead. CI practitioners will never learn how to "navigate the gray zone" by studying corporate compliance plans. The best "compliance plan" for CI professionals is to understand basic trade secret law.

D. The article "A Brief Compliance Manual," published in Competitive Intelligence Review [Vol. 9(1)] contains one glaring error regarding misrepresentation.

⁶The list of seven "must haves" from the Sentencing Guidelines, referred to in EEA compliance plan articles and presentations are not obligatory (i.e., "The organization must have established compliance standards and procedures . . . the organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents . . ."). The document is talking to the judge, not the corporate defendant. The corporate defendant "must have" taken these steps for the judge to find that a reasonable plan to "detect and prevent" crime was in place, not that the company "must have" done these things as an independent legal obligation.

⁶See the annual reports of the United States Sentencing Commission for a perspective on corporate and individual sentencing. The statistical data contained in the reports show, for example, that there were over 40,000 criminal sentences in federal courts in 1994, of which under 400 involved corporate defendants.

The article's "Fraud" section presents an MBA student who also works, who approaches his employer's competitor for an interview and introduces himself only as a student. Citing the section 529 of the Restatement of Torts, the article concludes that "Stating the truth in so far as it is misleading because a qualifying matter has been omitted, is a fraud."¹⁸

The article quotes other legal sources supporting the proposition that "If one speaks, 'he must disclose enough to prevent his words from being misleading' "¹⁹ and "It is now quite clear that a half truth is as bad as a lie."²⁰

It is incorrect to apply these legal sources to the MBA student hypothetical. A half-truth can be "as bad as a lie" when one is under a legal duty to tell the truth, such as the seller's obligation to the buyer in the context of a business transaction. True, section 529 of the Restatement explains that "A statement containing a half-truth may be as misleading as a statement wholly false," but continues "Whether or not a partial disclosure of the facts is a fraudulent misrepresentation depends upon whether the person making the statement knows or believes that the undisclosed facts might affect the recipient's conduct in the *transaction in hand*" (*emphasis added*). The Restatement offers examples such as a prospectus that accurately states assets but omits "any reference to its floating debt," "a statement by a vendor that his title has been upheld by a particular court is a false misrepresentation if he fails to disclose his knowledge that an appeal from the decision is pending," and "one who offers land or a chattel for sale on inspection by so doing impliedly asserts that he knows of nothing that makes the appearance of the article deceptive."

Prosser and Keeton similarly relate the "half-truth" rule to business transactions: "Merely by entering into some *transactions* at all, the defendant may reasonably be taken to present that some things are true," and cites as examples "turning back the odometer of an automobile offered for sale" or "stacking aluminum sheets to conceal corroded ones in the middle" (*emphasis added*).

True again, that Prosser and Keeton state: "... if the defendant does speak, he must disclose enough to prevent his words from being misleading," but cites as examples "the rental of a property which does not mention that it is illegal," or "the income of an amusement center which does not disclose that there has been a police raid which is likely to affect it."

The text from which "It is now quite clear that a half truth is as bad as a lie"²⁰ qualifies it with the following illustration: "Thus, in 1932 a British court sent Lord Kyl-

sant to prison because his steamship line had issued a prospectus that truthfully stated its average net income for the past ten years and its dividends for the past 17 years, but had deliberately concealed the fact that its earnings during the first three years of the ten years had been greatly augmented by World War I as compared with the seven lean years that followed."

To strengthen my analysis, I performed the following search: <res! /3 torts /5 529 and trade secret> of all federal and state cases on the Lexis system, which showed that there are no trade secret cases citing this section of the Restatement.

In short, the article presents the law of fraudulent misrepresentation without clarifying that it applies to situations where one has a legal duty to tell the truth, such as the seller in a business transaction.

THE LAW OF FRAUDULENT MISREPRESENTATION
APPLIES TO SITUATIONS WHERE ONE HAS A
LEGAL DUTY TO TELL THE TRUTH, AS THE
SELLER IN A BUSINESS TRANSACTION.

E. The purpose of Peter Kalitka's article "Are Competitor Intelligence 'Professionals' Trying To Have It Both Ways?" (CIR 9(3): 25-29) is apparently to warn the CI community to beware of people who argue that the EEA is necessary to combat efforts of those stealing American trade secrets and who are at the same time teaching CI professionals how to exploit weaknesses in their competitors.

This thesis can be dismissed by simply noting that because information collection techniques are aggressive does not necessarily make them illegal.

Mr. Kalitka also makes reference to the three-hour workshop I delivered on the topic of CI and the EEA at SCIP's 1998 Annual Conference by writing of "discussion forums designed to understand 'why the EEA of 1996 was never intended to apply to CI professionals'? Really? Doesn't the law apply equally to everyone under the jurisdiction of that law or are CI professionals to be given 'gray area' immunity?"

The exact reference in the convention brochure stated that I would "show why the EEA was never intended to apply to the CI profession." As I would expect one who understands the statement in its original to mean that identification as a CI professional allows for an exemption from a federal law to not be the sort to contemplate the practical significance of the EEA. I therefore conclude that Mr. Kalitka has for whatever reason significantly mischaracterized my presentation.

Perhaps most disturbing is Mr. Kalitka's critique that some CI professionals "skirted ethics" because they knew that "ethical rules were not policed or enforceable," this particularly in light of the fact that Mr. Kalitka actually criticized SCIP's Code of Ethics as being "so broad and so general, that in several cases it encourages a variety of interpretations."²¹

What comes to my mind is the following: *A* loans *B* his weapon. Does *B*'s ethical obligation to return *A*'s weapon to him apply even if *A* "subsequently went out of his mind?"—answered in the negative in *Republic* by Plato.²² Jump to the twentieth century, where in "*The Other America: Poverty in the United States*," Michael Harrington relates the following story: An employer knows that employee's drinking problem is so severe that one more bout with alcohol could kill him. Concerned that employee will purchase liquor, come pay day the employer decides nonetheless to pay the employee his earned wages, who spends it on alcohol and dies the following day from intoxication.

I cite these examples to demonstrate that questions which have been analyzed since human intellect first took an interest in ethics have relevance for contemporary situations, making the notion of policing ethics after discouraging other interpretations a dangerous one indeed.

THAT INFORMATION COLLECTION TECHNIQUES
ARE AGGRESSIVE DOES NOT NECESSARILY MAKE
THEM ILLEGAL.

Misapprehensions

I believe it is only a matter of time for the CI community to recognize that the initial public reaction to the EEA was based on misapprehensions rather than a reasoned understanding of trade secret law. Assertions such as the one made by "a large-firm California IP litigator, who spoke on the condition of anonymity" that he "suspect(s) that the [EEA] was pushed by out-of-work FBI people now that the Cold War has slowed down"²³ or that "industry has pushed hard for [the EEA] because it perceives a decline in employee loyalty"²⁴ will be looked back at as amusing.

As to how ideas take on a life of their own and become rumors, myths, or fears, see *Extraordinary Popular Delusions and the Madness of Crowds* by Charles Mackay (originally published in London in 1841), *The Natural History of Stupidity* by Paul Tabori (a serious piece of scholarship despite its name), and *The True Believer* by Eric Hoffer.

Perhaps, the most important lesson to be learned from this matter is that the ethical standard is more restrictive than the legal standard. Properly trained CI professionals who recognize what this standard means and have incorporated it into their business practice need not be distracted or concerned by the EEA debate.

Finally, I encourage those who disagree with any part of my analysis to critique or challenge it in writing.

Endnotes

1. "New Spy Law Could Cramp Economy," *USA Today*, February 20, 1997.
2. "New Spy Act to Boost White-Collar Defense Biz," *The National Law Journal*, July 28, 1997, p. A1.
3. "Go Directly to Jail: New Federal Law Protects Trade Secrets," *New Jersey Law Journal*, March 9, 1998, p. 32.
4. "U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance," *Business Crimes Bulletin*, January 1998, p. 4.
5. Fine, N. (February 1998) "The Economic Espionage Act: A Wake-Up Call," *SCIP 2nd Annual Symposia on Ethics and the Law Proceedings*, p. 15.
6. Fine, N. (February 1998) "The Economic Espionage Act: Turning Fear Into Compliance," *SCIP 2nd Annual Symposia on Ethics and the Law Proceedings*, p. 135; also *Competitive Intelligence Review*, 8(3):20.
7. "Economic Espionage Act: A Whole New Ball Game," *New York Law Journal*, January 2, 1997, p. 5.
8. Pooley, J. (Fall 1997) "Criminal Consequences of Trade Secret Theft: The EEA and Compliance Plans," *SCIP EEA Symposia Proceedings*; also *Competitive Intelligence Review*, 8(3):13.
9. Fine, N. *SCIP EEA Symposia Proceedings*, February 24–35, 1997, section 3, p. 18.
10. Economic Espionage Act of 1996: Implications and Protective Measures to be Addressed at CSI NetSec '97, *PR Newswire*, February 25, 1997.
11. See footnote a.
12. See Congressional Records of October 2, 1996, S12214.
13. Section 757, comment a.
14. *Defiance Button Mach. Co. v. C&C Metal Products*, 759 F.2d 1053, 1063–1064 (2d Cir. 1985).

15. *Franke v. Wiltseck*, 209 F.2d 493, 494-495 (2d Cir. 1954).
16. "Ex-Silicon Valley Executive Held in Plot to Steal Secrets," *The San Francisco Chronicle*, March 8, 1997; "Japanese Man Arrested On Corporate Spy Charges," *Agence France Presse*, March 8, 1997; "FBI Arrests Japanese Man On High-Tech Fraud Charges," *Reuters North American Wire*, March 8, 1997; "Man Posed As Toshiba Worker To Obtain Data, FBI Says," *Electronic Buyers' News*, March 17, 1997; "Ex-Linear Japan Exec Deported In Fraud Case," *Electronic News*, June 2, 1997.
17. "Atlantan In Corporate Spy Case," *The Atlanta Journal and Constitution*, May 10, 1997; "New River Textile Maker Accuses Big Rival of Spying," *Roanoke Times & World News*, May 16, 1997; *NRB Industries v. R.A. Taylor & Associates et al.*, Second Amended Complaint, No. 97 Civ. 0181, p. 43.
18. *Competitive Intelligence Review*, (9)1:31.
19. *Prosser and Keeton on Torts*, 5th ed., 1984, p. 738.
20. L. Loss and J. Seligman, *Securities Regulation*, 9A.2.
21. Kahika, P. (Fall 1997) "Counterintelligence and Law Enforcement: The Economic Espionage Act of 1996 versus Competitive Intelligence," *Competitive Intelligence Review*, 8(3):27.
22. Plato (1987) *The Republic*, p. 66, New York, Penguin Books.
23. "New Spy Act To Boost White-Collar Defense Biz," *The National Law Journal*, July 28, 1997, p. A18.
24. "Intellectual Property Concerns Overdone, Not Half-Baked" *Research-Technology Management*, March/April 1998.

About the Author

Richard Horowitz is an attorney concentrating in corporate, security, and international issues. He also holds a private investigator's license and served in the Israel Defense Forces with the rank of captain. He is a member of SCIP, and can be reached at 400 Madison Avenue, Suite 1411, New York, NY 10017; Tel: (212) 829-8196; Fax: (212) 829-8199; or e-mail RHESQ@Compuserve.com.

Industry spying still flourishes

Criminalizing trade secret theft hasn't led to mass prosecutions.

BY VICTORIA SLIND-FLOR
NATIONAL LAW JOURNAL STAFF REPORTER

WHEN THE federal Economic Espionage Act was signed into law in 1996, the Society of Competitive Intelligence Professionals got very nervous.

The new law criminalized the misappropriation of trade secrets, and members of the Alexandria, Va.-based organization conduct research and analysis on competitors to help their various companies plan strategy. Even before the act, they were hypersensitive about suggestions that their work is espionage or industrial spying.

So the organization brought in Richard J. Horowitz, a New York solo practitioner with a background in surveillance and security services. He prepared an analysis of the new law, concluding that its impact on legitimate competitive intelligence-gathering would be negligible.

Nearly four years later, it appears that Mr. Horowitz' predictions were on target. Criminal charges have been filed in only 21 still-pending cases to date. Surprisingly, only one of those arose in Silicon Valley. And instead of focusing on computer chips and software, many cases have involved lower-tech industrial products, including adhesives and pet food.

Nothing much changed

Many more investigations have been conducted without charges being filed, says Marc J. Zwillinger, a trial attorney at the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. And so far, "none of the cases have involved competitive-intelligence professionals."

The bottom line according to Mr. Horowitz: "If you weren't doing anything illegal beforehand, you aren't doing anything illegal now." Companies should not be quick to brag that they modified their intelligence-gathering rules in the light of the act, he says: "If you had to overhaul...then you weren't doing things legally."

Peter Toren, a partner at New York's Brown & Wood L.L.P., was working in the Justice Department when the act became law. He says one reason there have been so few cases is

that until late 2001, the Justice Department had to sign off on any prosecution. And many U.S. attorneys' offices "have a six or seven-figure loss requirement before they will even look at a white-collar case," he says. "Another factor is whether the victim has available a civil remedy."

James Pooley tried in vain to persuade one U.S. attorney to prosecute a trade secret case. "The guy had taken confidential information and was threatening to use it unless my client would negotiate a deal in his favor, and as he was saying this, he placed a gun on the table," Mr. Pooley said.

Mr. Pooley, a partner at Gray Cary Ware & Freidenrich L.L.P., of San Francisco and Palo Alto, Calif., said that even after he told the prosecutor about the gun, "his response was, 'Have you tried civil remedies?'"

"We're still working our way



Bodyguard: Richard Horowitz was hired to help industry avoid illegal actions.

through prosecutors' getting used to the criminalization of something that historically has not been criminalized," he said.

Criminal defense counsel Thomas J. Nolan, of Palo Alto's Nolan & Armstrong, suggests, however, that victims of trade secret theft are better served by the civil system.

To date, all prosecutions have fallen under Sec. 1832, on

commercial espionage. At first, most attention focused on Sec. 1831, which dealt with "agents of foreign power." "It was passed very quickly in an election year," said Mr. Pooley.

What started as an effort to address foreign states' involvement in espionage, he said, "morphed into a very broad statute addressing domestic theft as well." ■

THE NATIONAL LAW JOURNAL, May 29, 2000

Trade Secret Protection & Enforcement of
Intellectual Property Rights
28 November 2000

Business Intelligence: What drives the need?

William E. DeGenaro
DeGenaro & Assoc., Inc.



Corporate Learning

"The real race is to learn and the competition
will be won by those who create the
most valuable configurations of knowledge
in the shortest time."

Charles Hampden-Turner
Charting the Corporate Mind



"Superior military power in the future
depends on our ability to acquire and
process information faster than our
adversaries."

Admiral David E. Jeremiah
Vice Chairman of the Joint Chiefs of Staff

...we must maintain decision
superiority at all echelons and at
all nodes

VADM J.O. Tuttle, USN (Ret)

"We must get inside an
opponent's decision cycle."

At each of the war fighting echelons — strategic,
operational and tactical — US forces must have
enough information superiority to achieve
dominant battle space awareness — knowing
what opponents plan to do in a timely enough
fashion to counteract and defeat them.

Barbara A. Ducksworth
Vice Director for Operations
Defense Intelligence Agency



"Next to knowing all about your own business, the best thing to know about is the other fellow's business."

John D. Rockefeller

God Forgives Sinners,
but Stupid is Forever

Billy Sunday

"As business begins to compete on a more global scale, corporations, like national governments, are going to need intelligence systems. Those who use the product of intelligence will be better prepared to decide and to act."

Bob Galvin
Chairman, Motorola, Inc.

Characteristics of International Programs



- All major companies have organized BI programs
- Excellent collection with company-wide usage
- Government support in collection and industry dissemination
- Intelligence analysis, particularly forecasting, is weak



- Most major corporations have organized programs
- Professionally trained and managed departments
- Government and banking industry provide global support
- Senior management not BI educated, programs less effective

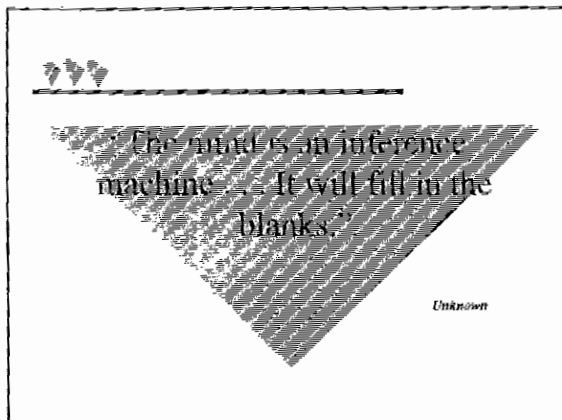


- Less than 5% corporations have fully developed BI systems
- Collection and analysis capabilities well-developed (SCIP)
- Government policy provides security, but not intelligence
- Not taught as management discipline in universities

American Management's Challenge

"Japan was defeated in world war II partly due to the superior intelligence and strategy developed by the Americans. Why can't Americans develop the same kind of intelligence and strategy to cope with Japan and be victorious? Most Japanese don't understand why American businessmen cannot win this war."

Japanese Ministry of International Trade & Industry (MITI)
1948 Press Conference



Spencer's Law of Data

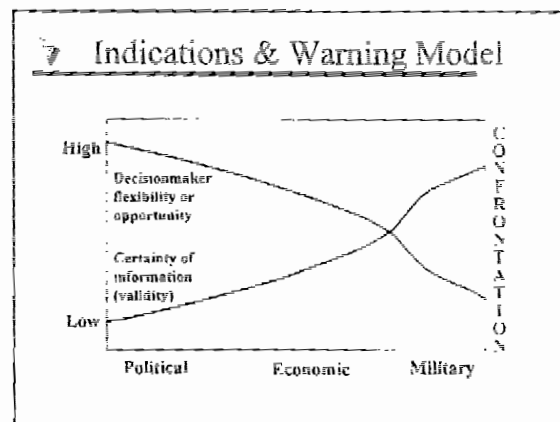
- Anyone can make a decision given enough facts
- A good manager can make a decision without enough facts
- A perfect manager can operate in perfect ignorance

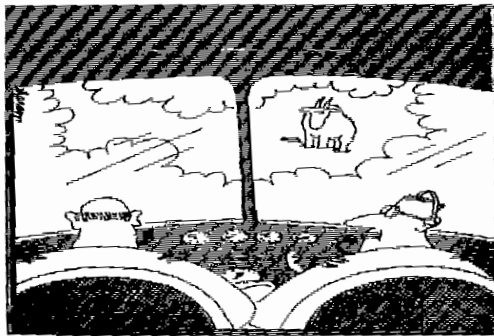
"No amount of sophistication is going to allay the fact that all your knowledge is about the past and all your decisions are about the future"

Ian E. Wilson, Chairman
General Electric

Uncertainty

the plague of all decision makers





"Say ... what's a mountain goat doing way up here in a cloud bank?"

Disasters are Potentially Foreseeable

- They were not created overnight
- During the incubation stage events accumulated which were at odds with norms



In no case had a lack of data
been a major factor in the
failure to anticipate the crisis.



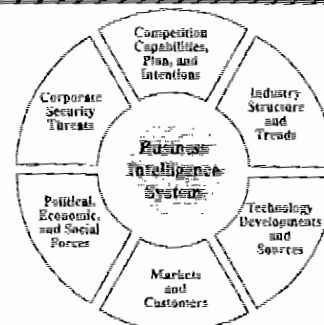
"The hallmark of a great
organization is how
quickly
bad news travels upward."

Jay Forrester

Boards of Directors and Senior
Management:

A duty to know?

BI Provides Comprehensive Coverage of the External Environment

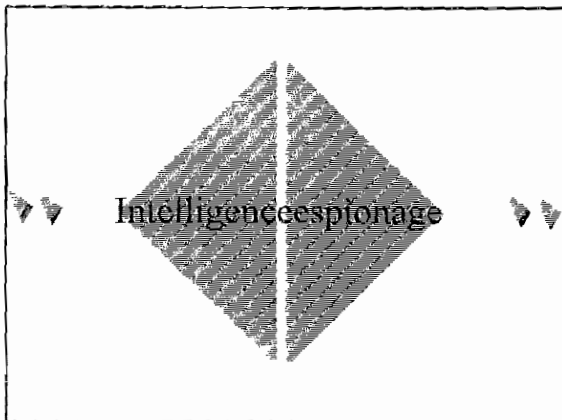


Primary Business Intelligence Functions

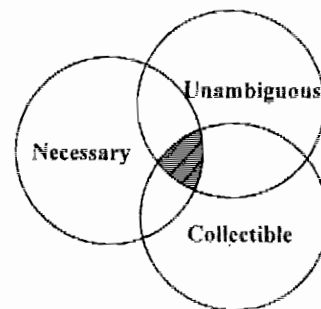
- Validate strategic assumptions
- Avoid surprise
- Map environment
- Predict future competition
- Consult on counterintelligence issues
- Educate consumers and practitioners

BR&A Products and Services

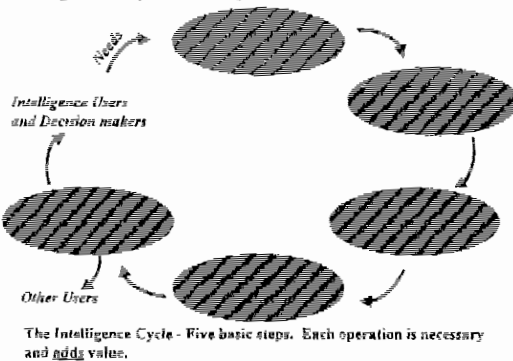
- Principal Corporate Competitor Monitoring and Analysis
- Regional and Industry Newsletters
- Threat Analysis
- Personality Profiles
- Key Customer Analysis
- Counterintelligence Consulting
- Business Unit BI System Support
- Benchmarking
- Acquisition Target Analysis
- Country Risk Analysis



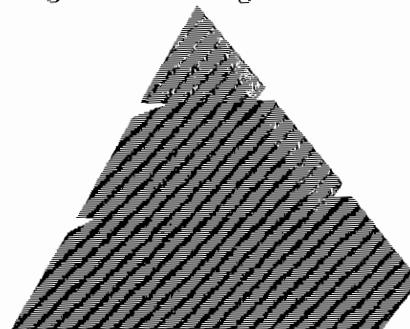
Useful Intelligence is . . .



Intelligence Systems Operations



Building the Knowledge Base





The ROI for business intelligence
is greater than the ROI for R&D.

Good Intelligence is an Investment . . . Not a Cost

- "Our Business Intelligence program is worth \$50M a year."
- "A single intelligence report led to an acquisition that contributes \$10M/year to our European Operations."
- "An intelligence assessment of our competitors' manufacturing facilities caused us to scrap our plans . . . and adopt a leading-edge production process."
- "Our competitors have beat us to the marketplace with similar products too often, and it has cost us millions."

Demonstrating the Need for Intelligence: A Case Study

Previous Decisions Gone Wrong

- Category pricing strategy
 - › \$400 million lost revenue potential
- European acquisition
 - › \$200 - \$300 million lost revenue potential
- Participation in government subsidies program
 - › \$200 - \$300 million lost revenue potential

Management Action: Develop an intelligence program

Demonstrating the Need for Intelligence: A Case Study

Future Decisions

- Pursue certain categories?
 - › \$100 - \$500 million revenue potential
- Better understand Latin American business opportunities
 - › \$200 - \$300 million revenue potential
- Leverage government program gains beyond contract terms
 - › \$ immeasurable revenue potential

Intelligence Supports . . .

Strategy . . .



*Strategy is Frustrated
for Lack of Intelligence*

☞ The lesson to be gained from this is that successful generals make plans to fit circumstances, but do not try to create circumstance to fit plans."

Patton

Competitive Decision Making

"... requires the focal actor to consider the contingent decisions of competitive actors."

Zajac & Bazerman
Northwestern University

Other Intelligence Consumers

- Investors
- Special interest groups
- Activists
- Suppliers
- Head hunters
- Financial analysts
- Distributors
- Researchers
- Consultants
- Foreign governments
- Trade groups
- Lobbyists
- Regulators
- Customers

"Counterintelligence ... is the key to the struggle between states and armies for a favorable disparity of knowledge."

Angela Casavola

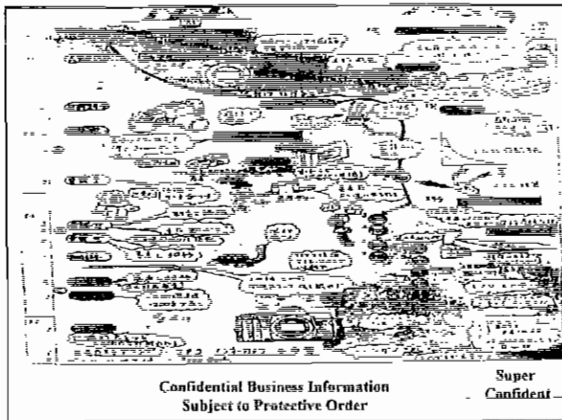
		Threat	
		Domestic	Foreign
Legal	Illegal		

Kempei Tai

"... Industrial espionage achieved a new pinnacle of respectability in Japan with the opening of the Institute for Industrial Protection, a school avowedly established to train spies and counterspies for Japanese corporations.

... This kind of intelligence work is regarded as patriotic and just as vital as military intelligence gleaned in time of war."

Richard Deacon



Ecole de Guerre Economique (EGE)

School of Economic Warfare

DeGenaro & Assoc., Inc.

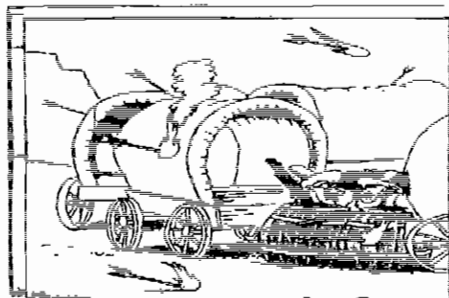
Ethics and Laws Supportive of Intelligence

"The French business intelligence system faces few pressures from lawmakers or from constituents: the wide popular consensus is that in matters of intelligence, morals and ethics do not apply. French companies do not maintain codes of ethics, perceiving them as an irrelevant Anglo-Saxon concept"

Jean-Marie Bonthous

Known Intelligence Attacks on 3M

Abrasive SBC	Sol gel and seeded gel technology in 1990
Consumer Group	Manufacturing technology in 1991
Reflective Products	New scouring pads manufacturing details
International	General business intelligence on market share, growth rates, operations in St. Paul and plants in 1991. Executive recruiting rooms.
3M West Coast	Briefcase of Joe Manager stolen at Inter-Continental Hotel in Paris
Orthopedic Prods.	Head hunters inquiries
COSD	3M plans for scratch cast
Tape Mfg.	Inquiries on Post-it [®] notes. Market size and growth rates, number of employees and square footage.
	3M's organizational structure, capacities and volumes



"Hey! They're lighting their arrows! ...
Can they do that?"

World Class Business Intelligence

- Targeted and Proactive
 - Focused on key intelligence topics
 - Avoids interference with currently effective mechanisms
 - Avoids information overload
 - Externally oriented
 - Concerned with the future
 - "Leading the target"

World Class Business Intelligence

- Driven by the needs of strategic decision makers
 - "Key Intelligence Topics"
- In the experience of TFG, these needs tend to fall into three categories:
 - Early Warning
 - Strategic Decisions or Issues
 - Key Players (competitors, others)

World Class Business Intelligence

- Begins with a *clear analytical framework* beginning with the needs of decision makers
 - Systematically *collects* necessary intelligence
 - First, from published sources and other *publicly available information*
 - Second, from a well-developed network of knowledgeable *human sources*
 - Seeks to generate *alternative hypotheses* to explain the observed phenomena
 - To avoid "groupthink" and "mirror imaging"
 - Fully *examines the implications* of the intelligence for the company and its decision makers
 - Thus generating follow-up questions for the intelligence unit

DeGenaro & Associates, Inc.
1133 4th Street
Suite 200
Sarasota, FL 34236

Theft of Trade Secrets

Joseph C. Metcalfe
Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice
(202) 514-1026

Topics Covered

- I. EEA Statutory Review
- II. EEA Case History and Approvals
- III. Advice to Industry

I. EEA Statutory Review

Need for Legislative Reform

- Recognition that information is often a corporation's most valuable asset
- Threat of foreign misappropriation
- Theft of proprietary information increasingly common
 - \$151 million loss in 2000 from 186 companies surveyed, according to the 2001 Computer Crime and Security Survey
- Other criminal statutes not always helpful
 - Mail and Wire Fraud (18 U.S.C. §§ 1341, 1343) limited to cases involving mail or wire transmissions, requires scheme to defraud
 - Interstate Transportation of Stolen Property Act (18 U.S.C. § 2314) limited to theft of tangible property (*United States v. Brown*, 925 F.2d 1301 (10th Cir. 1991))

Toren footnote 1

Scope of the EEA

- Codified at 18 U.S.C. §§ 1831-1839
 - Effective October 11, 1996
 - Federally criminalizes the theft of trade secrets
- § 1831: theft of trade secret to benefit a foreign government, instrumentality or agent
 - No prosecutions since EEA became law
- § 1832: general theft of trade secrets
 - By outsider or insider, foreign/domestic company or individual
 - Charging an EEA violation requires approval by Attorney General (28 C.F.R. § 0.64-5)
 - Approval requirement expires October 11, 2001

Statutory Scheme

- § 1831: Foreign economic espionage
- § 1832: Theft of trade secrets
- § 1834: Forfeiture provision
- § 1835: Confidentiality provision
- § 1836: Civil enforcement
- § 1837: Conduct outside the United States
- § 1839: Definitions

Elements of an 1832 Violation

- 1. Defendant stole, or without authorization of owner, obtained, destroyed, received or conveyed information
- 2. Defendant knew or believed information was a trade secret
- 3. Information was in fact a trade secret.
- 4. Defendant intended to convert the trade secret to the economic benefit of someone other than owner
- 5. Defendant knew or intended that the owner of the trade secret would be injured
- 6. Trade secret was related to a "product" that was produced for or placed in interstate or foreign commerce

Comparison of §§ 1831 and 1832

- | | |
|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| • 1. Defendant misappropriated information | • 1. Defendant misappropriated information |
| • 2. Defendant knew information was a trade secret | • 2. Defendant knew information was a trade secret |
| • 3. Information was a trade secret | • 3. Information was a trade secret |
| • 4. Defendant knew/intended that the offense would benefit a foreign government, foreign instrumentality or foreign agent | • 4. Defendant intended to convert the trade secret to the economic benefit of someone other than owner |
| | • 5. Defendant knew/intended that owner would be injured |
| | • 6. Product in interstate or foreign commerce |

Definition of Trade Secret: § 1839(3)

- § 1839(3): "The term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if ...

Definition of Trade Secret (cont.):

§ 1839(3)

- § 1839(3) (continued):
 - (A) the owner thereof has taken reasonable measures to keep such information secret; and
 - (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."
- Broader than the Uniform Trade Secrets Act
 - UTSA enacted in most states, provides victims of trade secret theft with a private cause of action
 - Definition in UTSA: "Information, including a formula, pattern, compilation, program, device, method, technique, or process..."
 - Courts have applied the UTSA to many types of information, similar to the BEA definition

Dont like
default passwords

Definition of Trade Secret (cont.): Secrecy/ "Reasonable Measures"

- Think in terms of physical world and cyberspace:
 - Building security
 - Network security, including password protection and encryption
- Confidentiality agreements often critical
- Disclosure to third-parties should be under controlled circumstances (e.g., non-disclosure agreements)
- Measures taken by owner should be commensurate with the value of the trade secret
- Security measures need to be absolute, but reasonable under the circumstances
- Trade secret can include elements in the public domain

Definition of Trade Secret (cont.): "Independent Economic Value"

- Value must derive from the information not being known to the public
 - Possible examples include source code, manufacturing plans, unique processes, design specifications
- Customer list example:
 - Not a trade secret if
 - customers widely known in particular industry
 - list merely the result of general marketing efforts
 - the information is easily ascertainable
 - list includes nothing more than contact information
 - Potentially a trade secret if
 - difficult or impossible to discover customer information through public sources
 - list created through substantial expenditure of time and money
 - information goes beyond names and phone numbers

Definition of Trade Secret (cont.):

Limitations

- Fundamental concept:
 - “Section 1832(a) was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It was, however, designed to prevent those employees ... from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere.” *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000).
 - EEA does not criminalize use of general skills or parallel development of a similar product
- Although broadly defined, “trade secrets” does not include all information a business might consider proprietary

Review of Elements - Misappropriation

- Central concept: activity without consent of owner that diminishes value of the information = misappropriation
- Acts prohibited include traditional instances of theft (i.e., item or object removed from the owner's possession)
- EEA extends definition of “misappropriation”
 - Includes copying, distributing, photographing, downloading, sending, and receiving
 - Such actions in the context of trade secrets may reduce or destroy the value of the property

Review of Elements - Knowledge That Information Was Trade Secret

- Gov't must prove that the defendant knew or had a firm belief that the information “misappropriated” was a trade secret
- Related to measures owner took to keep information secret and why the information was valuable because not generally known to the public (§ 1839(3))
- Statements of defendant often critical

Review of Elements - Information Was A Trade Secret

- When charging theft, duplication, transmission, receipt or possession, the "misappropriated" information must in fact be a trade secret
- However, if charge is attempt or conspiracy, government need not prove existence of actual trade secret (United States v. Hsu, 155 F.3d 189 (3rd Cir. 1998))

Review of Elements (§ 1832) - Intent To Benefit Economically

- Gov't must prove defendant intended to convert the trade secret to the economic benefit of someone other than owner
- Benefit can flow to any third party, not just the defendant
- Must be economic benefit
- Acting solely out of malice/revenge/spite not enough

Review of Elements (§ 1832) - Intent To Injure Owner

- Gov't must prove defendant knew or intended that actions would cause some disadvantage to the rightful owner
- Often this element satisfied circumstantially with evidence of intent that someone other than owner benefits economically
- Sometimes intent to benefit does not support inference of intent to injure (e.g., defendant wishes to compete in foreign market that will have no effect on owner's business)

Review of Elements (§ 1832) - Related to Product In Commerce

- Gov't must prove trade secret was related to a "product" that was produced for or placed in interstate or foreign commerce
- Distinction between a pure service and a product not always clear
 - Doctor's unique method of treating patients, if not related to the development of a medical product, likely not protected by the EEA
 - Many "services" are in fact sold much like products and would likely be consider a product under the EEA (e.g., cellular telephone services, credit card services)

Affirmative Defenses

- Parallel development
- Reverse engineering
- Advice of counsel in bona fide dispute about ownership of intellectual property

Sentencing Considerations

- § 1831 maximum penalties:
 - 15 years and/or \$500,000 fine for individuals
 - \$10,000,000 fine for corporations
- § 1832 maximum penalties:
 - 10 years and/or \$250,000 fine for individuals
 - \$5,000,000 fine for corporations
- Actual sentences have ranged from probation to 77 months imprisonment
- Covered under USSG 2B1.1 (Theft)

Sentencing Considerations (cont.) -

2B1.1

- Base level of 4
- +2 for more than minimal planning
- +2 if defendant knew or intended offense to benefit foreign government, instrumentality or agent
- Increase offense level based on amount of "loss"
 - Loss greater than \$10,000 = +5
 - Loss greater than \$800,000 = +13

Sentencing Considerations (cont.) -

Loss Calculations

- Loss need not be determined with precision
- § 1832 loss calculations:
 - Loss = "fair market value of the property taken, damaged, or destroyed"
 - The amount the trade secret was sold for, or
 - "Reasonable Royalty" or "Forced licensing" - amount buyer would have paid if had he legitimately licensed the stolen technology
 - Gain to defendant measured by amount defendant would have had to invest to develop independently, usually measured by victim's historical R&D costs
- If market value difficult to ascertain or inadequate to measure harm, court may measure loss another way (e.g., reasonable replacement cost to victim)

Additional EEA Provisions

- Criminal forfeiture (§ 1834)
 - Court shall order the forfeiture of any proceeds or property derived from violations of the EEA
 - May order the forfeiture of any property used to commit or facilitate the commission of the crime (proportional to the crime)
- Confidentiality (§ 1835)
 - Court shall take such actions to preserve the confidentiality of trade secrets
 - Government has right to bring interlocutory appeal authorizing disclosure of trade secret
 - Failure to cooperate with EEA prosecution often related to fears of disclosure

Additional EEA Provisions (cont.)

- Civil Proceedings (§ 1836)
 - Government (not private party) can file a civil action for an injunction to preserve status quo during criminal investigation
- Extraterritoriality (§ 1837)
 - Applies to conduct occurring outside U.S. if
 - the offender is a citizen or permanent resident alien of the U.S.; or
 - an act in furtherance of the offense was committed in the U.S.

II. EEA Case History and Approvals

27 EEA Cases To Date

- How we learn of EEA violations:
 - Competitor reports it
 - Victim company suspects insider
 - Insider reports outside contact
 - Victim complains of competing product
- Wide variety of circumstances forming basis of EEA charge:
 - Insider + buyer cooperating
 - Buyer only seeking seller of trade secret
 - Direct theft
 - Seller shops secret around to potential competitors

Factors Influencing Government Decision To Prosecute

- Is the gov't being dragged into civil case?
 - Are civil remedies adequate?
- What type of information was misappropriated?
 - Scientific and research information easier to value
- Satisfies product requirement?
- How valuable is the proprietary information?
 - USAO's monetary guidelines for fraud/theft cases
 - Victim-generated estimates closely scrutinized

Factors Influencing Government Decision To Prosecute (cont.)

- Is the information clearly a trade secret?
 - Did the owner take "reasonable measures"?
 - Does the information have "independent economic value"?
- Is the information in the public domain?
 - Sub-contractors or licensees? Scientific articles? Patents filed?
- Is there evidence of theft and consciousness of guilt?
 - Won't rely solely on emergence of a similar product
- Is the victim cooperative?
 - Promptly reported? Would prosecution jeopardize the confidentiality of the trade secret?

III. Advice to Industry

Don't be a victim or a target

- Protect your trade secrets, whether stored on paper or electronically
- Have systems in place to prevent your company from being victimized
 - Physical and cyber security measures (encryption, strong passwords), background checks, limited access to key secrets
 - Confidentiality and non-disclosure agreements
 - Use physical security, background checks, limited access to key trade secrets
- Educate employees about the EEA
- Watch the information offered by or received from new employees hired from competitors

If you think you are a victim...

- Find out information in a manner that keeps your options open
 - Internal investigation
 - Investigative firm
- Don't resort to self-help
- Determine whether to handle the matter internally, bring a civil suit, or refer to the FBI

Refer the case to the FBI?

- Pros:
 - Powerful message to would-be corporate predators
 - Effective, inexpensive discovery
 - Restitution available
 - Liability can be established
- Cons:
 - Gov't will not take border-line cases
 - May delay or impede civil case
 - Requires cooperation of victim
 - Cede control to government
 - Some risk of exposing trade secrets

Where to get more information

- Computer Crime Website:
 - www.cybercrime.gov
 - Table of EEA cases, press releases
- "Federal Prosecution of Violations of Intellectual Property Rights: Copyrights, Trademarks, and Trade Secrets"
- Call CCIPS

Federal Prosecution of Thefts of Trade Secrets Under the Economic Espionage Act of 1996

By Peter J. Toren*

[a] Introduction

In recent years the scope of economic espionage in the United States has greatly increased,¹ especially with the end of the Cold War, which has redefined the context for espionage as a nation's security becomes more closely linked to economic prosperity.² However, until recently, federal prosecutors were limited in their ability to prosecute even the most egregious theft of trade secrets because there was no federal law that was designed to cover such activities.³ In response to this shortcoming in federal criminal law, and in recognition of the increasingly vital role

*The author is a partner and co-head of the Intellectual Property Group of Brown & Wood LLP where he specializes in IP litigation. He is also an adjunct professor of law at Hofstra University where he teaches a course in Cyberlaw. Before entering private practice, Mr. Toren was a Trial Attorney with the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, where he helped draft the Economic Espionage Act, prosecuted violations of copyright, trademark and trade secret laws, and co-authored *Federal Prosecution of Violations of Intellectual Property Rights (Copyrights, Trademarks and Trade Secrets)*.

¹ A survey released in 1996 by the American Society for Industrial Security (ASIS) showed a 323% increase in incidents involving the theft of trade secrets from 1992 to 1995 and an estimated annual loss to U.S. companies of \$25 billion. Business Week, July 14, 1997 at 76

² FBI Director Louis Freeh testified that as a legacy of the Cold War, at least 23 foreign countries have targeted acquiring trade secrets from U.S. companies. Senator Herbert Kohl of Wisconsin has asserted:

Even as the cold war ended, our former enemies and our current allies began retooling their intelligence agencies. They have turned their vast spying apparatus on us, on our businesses, on the very ideas and information that keep this country safe . . . Foreign governments look at America and see a one-stop shopping mall [for business information], and what they cannot buy legitimately, they will shoplift.

"The Industrial Espionage Act and the Economic Security Act," Federal Document Clearing House, Congressional Hearings Summaries, February 28, 1996.

³ In particular, prosecutors attempted to use the Depression-era Interstate Transportation of Stolen Property Act, 18 U.S.C.A. § 2314, and the Wire Fraud and Mail Fraud statutes, 18 U.S.C.A. §§ 1343 and 1341, respectively. For an excellent discussion of the limitations of Federal laws prior to the passage of the Economic Espionage Act in dealing with the thefts of trade secrets, see James Pooley, Mark Lemley, and Peter Toren, "Understanding the Economic Espionage Act of 1996," 5 Tex Intell. Prop. L.J. 177 (Winter 1997).

intellectual property, in general, and trade secrets, in particular, play in the U.S. economy, Congress enacted the Economic Espionage Act of 1996 ("EEA").⁴ The EEA, for the first time, makes the theft of trade secrets a federal crime.⁵ Further, while the EEA is clearly intended to mainly apply to criminal conduct committed within the United States, it includes a very broad and far-reaching extraterritorial provision that may impact foreign companies that do business in the U.S. and U.S. companies that do business abroad.⁶

Given the broad reach of the EEA and given that a conviction for a violation of the EEA could subject an individual to imprisonment for up to ten or fifteen years and a corporation to a fine of up to \$10 million⁷ and could result in the forfeiture of part or all of the property used to facilitate the theft,⁸ it is imperative that corporate officers and all employees have a general understanding of the scope and coverage of the EEA. Conversely, in order to better protect trade secrets from theft, it is also important for victims of trade secret thefts to understand when it is appropriate to refer an alleged theft of trade secrets to the federal government for investigation and criminal prosecution.

This section analyzes the scope of the EEA, and provides a summary of some of the EEA prosecutions that the government has brought to date. It also discusses the substantive and procedural aspects of making a criminal referral and the advantages and disadvantages of criminal prosecution. Finally, the discussion focuses on steps a corporation can take to avoid becoming a defendant in an EEA prosecution and how to minimize corporate liability through the implementation of a corporate compliance plan.

⁴ Economic Espionage Act of 1996, Pub. L. No. 104-294, Title I, § 101(a), 110 Stat. 3488 (codified at 18 U.S.C.A. §§ 1831-1839).

⁵ Prior to the passage of the EEA, there was only a single, very limited federal statute that directly prohibited the unauthorized disclosure of government information, including trade secrets, by a government employee. 18 U.S.C.A. § 1905. Its impact is further limited because it provides for only misdemeanor criminal sanctions.

⁶ 18 U.S.C.A. § 1837.

⁷ 18 U.S.C.A. §§ 1831, 1832.

⁸ 18 U.S.C.A. § 1834.

[b] Overview of the EEA

[i] Prohibited Conduct

The EEA contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision, codified at 18 U.S.C.A. § 1831, covers thefts of trade secrets that are intended to benefit a foreign government, instrumentality or agent.⁹ Thus, this section covers true “economic espionage.” In contrast, 18 U.S.C.A. § 1832 makes criminal the more common commercial theft of trade secrets, regardless of who benefits.

In order to prove a violation of § 1832, the government must prove beyond a reasonable doubt that:

- (1) The defendant stole, or, without authorization of the owner, obtained, destroyed or conveyed information;
- (2) The defendant knew this information was proprietary;
- (3) The information was in fact a trade secret;
- (4) The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;
- (5) The defendant knew or intended that the owner of the trade secret would be injured; and
- (6) The trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

Section 1832 also explicitly criminalizes attempts and conspiracies to engage in espionage and steal trade secrets.¹⁰ According to a recent Third Circuit decision, the “government can satisfy its burden under § 1832(a)(4) [attempts] by proving beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such.”¹¹ This is important because it allows the government not to have to

⁹ Because prosecutions under this section probably will be extremely rare (in fact, to date, the government has not charged a single violation of this section), this article will not discuss this section in any further detail. For a complete description of the element of this section, see *Federal Prosecution of Violations of Intellectual Property Rights, Copyrights, Trademarks and Trade Secrets*, United States Department of Justice, May 1997.

¹⁰ 18 U.S.C.A. §§ 1831(a)(4), (a)(5) and 1832(a)(4), (a)(5).

¹¹ *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998).

use actual trade secret information in sting operations. This ruling should encourage victims of trade secret thefts to report the matter to the government for prosecution because it lessens the chances that a referral will inevitably result in further disclosure of the trade secret.

The EEA also makes criminal the knowing receipt, purchase, or possession of a stolen trade secret.¹²

[ii] Misappropriation

The type of acts that are prohibited under § 1832 are broadly defined and include traditional instances of theft, i.e., where the object of the crime is physically removed from the owner's possession.¹³ The section, however, also includes methods of misappropriation where the original property never leaves the custody or control of the owner, but the value of the trade secret to the owner may be effectively destroyed by the unauthorized duplication or disclosure to a third party. It has also been suggested that because this section is not, by its terms, limited to secrets acquired by "improper means," an individual can still theoretically violate the EEA even if the trade secret was acquired by proper means.¹⁴

The government must also prove that the defendant acted "without authorization" from the owner. This refers to whether, for example, the defendant had the consent of the owner of the trade secret to "copy . . . communicate, or convey a trade secret." Thus, for example, where an employee has authorization from his employer to copy a trade secret during the regular course of his employment, he can still violate the EEA if he "communicates or

¹² 18 U.S.C.A. §§ 1831(a)(3), 1832(a)(3).

¹³ Section 1832(a) punishes any individual who:

- (1) steals or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice or by deception obtains a trade secret;
- (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
- (3) receives, buys or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization . . .

¹⁴ See "Understanding the Economic Espionage Act of 1996" at 195.

conveys" the trade secret to a competitor without his employer's permission.

[iii] Knowledge

The government must also prove that the misappropriation was done knowingly. It must show that the defendant knew or had a firm belief that the misappropriated information did not belong to him.¹⁵ A person who takes a trade secret because of ignorance, mistake or accident does not violate the EEA.

[iv] Trade Secret Defined

The term "trade secret" is defined in the EEA as follows:

(3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public¹⁶

Thus, the definition of a trade secret under the EEA is extremely broad and encompasses information in any form "whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing." The references to intangible information and the "whether or how" language mean that not only information stored in electronic form but also information "stored" only in an individual's memory, can be the subject of prosecution for theft of trade secrets. It is noted, however, that although the EEA does theoretically cover thefts committed by memorization, because of the difficulty in establishing the defendant's criminal

¹⁵ 142 Cong. Rec. S12202, 12213 (daily ed. Oct. 2, 1996).

¹⁶ 18 U.S.C.A. § 1839(3).

intent in such a case, it is extremely unlikely that the government would prosecute a case in which there is no tangible evidence of theft.

One issue, however, that is not addressed by the EEA is the specificity with which the trade secret must be identified. Under civil trade secrets law in many states, plaintiffs may file a complaint and even proceed to trial without ever having specifically identified the trade secret they claim was stolen. By contrast, the legislative history suggests that “particularity” in describing trade secrets will be important under the EEA.¹⁷ In *United States v. Hsu*,¹⁸ the trial court denied the government’s motion for entry of a protective order preventing defendants from reviewing the documents allegedly containing trade secrets that were the subject of the government sting operation. The court chose instead to adopt a protective order providing for limited disclosure of the secrets to defendants’ attorneys, outside experts and prospective witnesses. The court reasoned that the failure to permit the defendants’ from having access to such documents would violate their Due Process and jury rights under the Fifth and Sixth Amendments on the ground that “the Government must prove under the plain language of the statute that a ‘trade secret’ existed within the meaning of the Act” and the government’s proposed protective order would relieve the government of this burden.

However, on appeal, the Third Circuit held that the trial court’s ruling was based on the erroneous understanding that the indictment charged the defendants with a completed theft when only attempt and conspiracy were charged. Because attempt and conspiracy do not require proof of the existence of a trade secret, the defendants “have no arguable right to view the unredacted portion of the . . . documents in order.”¹⁹ The court emphasized that to require otherwise would have the “bizarre effect of forcing the government to disclose trade secrets to the very persons suspected of trying to steal them, thus gutting enforcement efforts under the EEA. We believe Congress could not have intended such a result, inasmuch as it was striving to prevent economic

¹⁷ 142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996).

¹⁸ *United States v. Hsu*, 40 F. Supp. 2d 623, 50 U.S.P.Q.2d 1659 (E.D. Pa. 1999).

¹⁹ *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998); *see also* *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000) (relying on *Hsu* the court held that attempt and conspiracy to steal trade secrets do not require proof of the existence of a trade secret, but rather, proof only of one’s attempt or conspiracy with intent to steal a trade secret).

espionage and to maintain confidentiality of trade secrets.”²⁰ As noted above, this is an important ruling because it permits the government not to have to use the actual trade secrets in an undercover or sting operation.

[v] Economic Benefit

The EEA also requires that the government prove that the act of misappropriating the trade secret was intended by the defendant to economically benefit a person other than the rightful owner of the trade secret (which can be the defendant or some other person or entity). In other words, the EEA does not cover a situation in which a person acts for reasons other than the expectation of economic gain, such as for revenge or spite.²¹ This requirement is surprising since it is obvious that the extent of the injury to a trade secret owner does not depend on the motivation of the person who misappropriated the trade secret.

[vi] Intent to Injure the Owner of the Trade Secret

The government must also prove a third *mens rea* element: that the defendant intended to “injure” the owner of a trade secret. According to the legislative history, this provision “does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner.”²² It is unclear why Congress included this element in the EEA, since, although it is theoretically possible, it is extremely unlikely that a person could misappropriate a trade secret to benefit another without regard to the consequences for the trade secret owner. It is axiomatic that when a defendant misappropriates a trade secret, the owner of the trade secret is injured because he no longer has exclusive control over the trade secret. In *United States v. Martin*,²³ the 1st Circuit held that the government proved this element by establishing that the defendant intended to use the trade secrets to create a “more successful competitor with greater capability to injure the [victim].”

²⁰ *Id.* at 13

²¹ See, e.g., *United States v. LaMacchia*, 871 F. Supp. 535, 541-42 (D. Mass. 1994) (holding that the criminal copyright statute did not apply to an electronic bulletin board owner who posted infringing computer software without receiving any financial benefit).

²² H.R. Rep. No. 788, 104th Cong., 2d Sess. 1996.

²³ 228 F.3d 1 (1st Cir. 2000).

[vii] Interstate or Foreign Commerce

To constitute theft of trade secrets, the stolen secret must relate to, or be included in, a product that “is produced for or placed in interstate or foreign commerce.” This requirement raises two important questions concerning the scope of the EEA’s coverage: (1) whether the EEA is intended to exclude trade secrets relating to services as opposed to products; and (2) whether it applies to products that are intended to enter, but are not yet in, interstate or foreign commerce.

The answer to the first question is important to service companies such as advertising agencies, brokerages, financial service firms, and other companies that sell their expertise and rely on proprietary information, but do not sell products. Such information can be just as valuable as information relating to a new product. Given the importance of service industries to the American economy, it is unlikely that Congress intended to intentionally exclude from EEA coverage trade secret information relating to services. However, the matter has not been litigated and it is possible that a court when faced with this issue would reach the opposite conclusion.

The answer to the second question, to wit, whether the EEA applies to secrets relating to products that are not yet in interstate or foreign commerce is also extremely important because if the EEA does not cover such items, much of its protection would be lost. A trade secret is often most valuable during the research and development phase before the product has been released to the public and the trade secret can be discovered through legal means such as by reverse engineering. It is extremely unlikely that Congress would have intentionally excluded from coverage very valuable trade secrets that are related to products under development.²⁴ However, as is the case with the question of services described above, this issue has not been litigated and it is possible that a court when faced with this issue would find that the EEA does not cover the trade secrets relating to products in their development or research phase.

Further, this requirement also raises the question of whether the EEA protects “negative know-how,” that is, information, often gained only after substantial expense, about

²⁴ *The Prosecution Manual* takes this view, stating that “in cases in which the trade secret is related to a product still being produced but will ultimately be sold in interstate commerce, prosecutors should establish this fact, and argue it sufficiently meets this element.” *Prosecution Manual* at 80.

what doesn't work. Such information has been accorded protection as a trade secret under civil law.²⁵ Since negative know-how concerns only a product that relates to, or is included in, a product that "is produced for or placed in interstate or foreign commerce" to the very limited extent of how not to make that product, it is unlikely that the EEA protects this valuable information.

[c] Protection of Secrets

In enacting the EEA, Congress recognized that victims of trade secret thefts are often faced with a dilemma when deciding whether to report the matter to law enforcement authorities.²⁶ As the Department of Justice publication *Federal Prosecution of Violations of Intellectual Property Rights (Copyrights, Trademarks and Trade Secrets)* ("Prosecution Manual") notes, "victims do not want the thief to go unpunished but suspect if they report the matter, the trade secret will be publicly aired during criminal prosecution."²⁷ Section 1835 of the EEA attempts to answer this legitimate concern by providing that a court will establish safeguards to protect the trade secrets:

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United

²⁵ See, e.g., *Metallurgical Indus. Inc. v. Fourtek*, 790 F.2d 1195, 1198 (5th Cir. 1986) ("Knowing what not to do often leads automatically to knowing what to do."); *Nilssen v. Motorola, Inc.*, 963 F. Supp. 664 (N.D. Ill. 1997) ("Indeed, Motorola might face liability for misappropriation under [the Illinois Trade Secrets Act] even if it used Nilssen's trade secrets 'only to demonstrate what pitfalls to avoid'."). But see, *SI Handling v. Heisley*, 753 F.2d 1244 (3d Cir. 1985), rejecting the argument that such information was protectable, at least under the facts as presented.

²⁶ The House Judiciary Committee's section-by-section analysis with respect to § 1837 states that:

[t]he intent of this section is to preserve the confidential nature of the information and, hence, its value. Without such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth.

H.R. Rep. No. 104-788, at 13 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4032.

²⁷ *Prosecution Manual* at 83.

States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

The victim also can take a number of steps in an attempt to limit the scope of the disclosure of the trade secret. First, if the victim is assisting the government in a "sting" operation, the victim should provide the government with the type of trade secret information for use during the operation that will not cause harm if it is disclosed to the defendant.²⁸ This can be accomplished by providing the government with a patent application containing a trade secret²⁹ or with a trade secret that inevitably would be publicly disclosed anyway. In many respects, the former option is preferable because the information contained in the patent application will be accorded full protection after the patent issues, regardless of whether it is disclosed during litigation. In the alternative, the victim should encourage the government to charge the defendant with attempt or conspiracy, because as the court found in *United States v. Hsu*, that if a defendant is charged with attempt or conspiracy and not with a completed act, the defendant has no constitutional or statutory right to view the "unredacted portion of the . . . documents"

Second, the victim must also educate the federal prosecutor on the value and importance of the trade secrets involved and the great harm that the victim will suffer from any further disclosure. Third, after the defendant has been indicted, a trade secret owner should carefully monitor any proposed protective orders and seek to provide input into the scope and form of such orders. Finally, the victim should also encourage the prosecutor to take an interlocutory appeal from an order authorizing or directing the disclosure of any trade secret, as is permitted by § 1835.³⁰

²⁸ So-called "sting operations" are of most value in a matter in which the trade secrets have not yet been appropriated by the defendant or revealed to unauthorized competitors. In other words, the government sets up an operation with the intended victim's cooperation before the defendant has had the opportunity to misappropriate the trade secret. Sting operations have long been used by the government to combat illegal drugs with a great deal of success. *See, e.g., United States v. Everett*, 700 F.2d 900, 908 (3d Cir. 1983).

²⁹ Prior to December of 1999, patent applications remained secret until the PTO granted the application. Now, applications are published 18 months from filing date unless the applicant states that he or she does not have an intent to file outside the U.S. Under these circumstances the application remains secret.

³⁰ As described above, the permissible scope of a protective order has already been litigated in *United States v. Hsu*, and the United States has appealed the trial court's decision not to adopt the government's suggested protective order that permitted the court to redact trade secrets *in camera*, and

[d] Statutory Penalties

Reflecting the seriousness with which Congress viewed thefts of trade secrets, the EEA provides for strong penalties. Specifically, individual defendants convicted of violating § 1832 can be sentenced to up to ten years in prison³¹ and can be fined up to \$250,000.³² Corporations or other organizations that violate § 1832 can be fined up to five million dollars. Further, courts have respected Congress' intent and have sentenced individuals convicted under the EEA to stiff sentences:

- Patrick Worthing was sentenced to fifteen months in prison for stealing trade secrets from Pittsburgh Plate Glass ("PPG"). His brother Daniel, a PPG supervisor to whom Patrick had promised \$100 for assisting him, was sentenced to five years' probation with a special condition of six months' home detention.³³

- Steven Davis was sentenced to twenty-seven months and ordered to pay \$1.2 million in restitution to Gillette after pleading guilty to five counts of stealing trade secrets relating to the next generation of Gillette shavers.³⁴

- Mayra Justine Trujillo-Cohen, who admitted to offering for sale a proprietary computer program owned by Deloitte & Touche, was sentenced to forty-eight months' imprisonment and ordered to pay \$337,000 in restitution.

- The circulation manager for the Gwinnett Daily Post, Carroll Lee Campbell, Jr., was sentenced to three months' imprisonment and four months' home confinement for offering to sell confidential circulation information to the Atlanta Journal-Constitution.

instead adopted the order suggested by the defendants that permits the dissemination of such materials to defendants' attorneys, outside experts and prospective witnesses.

³¹ 18 U.S.C.A. § 1832(a).

³² Because the EEA does not specify the fine amounts for individuals, the amounts are determined under § 3571.

³³ "15 Months for Selling Secrets," Pittsburgh Post-Gazette (June 6, 1997). *See also* "Corporate Spies Feel a Sting," Business Week, July 14, 1997; "Industrial Espionage," Pittsburgh Post-Gazette (April 19, 1997).

³⁴ The Boston Globe (April 30, 1998) at E16.

[e] Remedies

[i] Civil Proceedings

In addition to penal and monetary penalties, § 1836(a) authorizes the government to file a civil action seeking injunctive relief.³⁵ In a small number of cases, the availability of this remedy could be important because the section would permit the government to use its injunctive power during the initial stages of a prosecution to maintain the status quo or prevent public disclosure of a victim's secret. Or in some circumstances where the defendant's conduct does not rise to the level of a criminal violation, civil injunctive relief may prove to be an appropriate substitute for criminal punishment. However, as has been pointed out, § 1836 adds little to the EEA.³⁶ Further, from a practical standpoint, because most Assistant United States Attorneys are unfamiliar (and uncomfortable) with civil law, they will not actively seek to use this section. Given these limitations, it is not unsurprising that there are no reported instances of the government seeking injunctive relief under § 1836.

[ii] Criminal Forfeiture

Section 1834 provides that the court in sentencing "shall order" the forfeiture of "any property constituting, or derived from, any proceeds the person obtained, directly or indirectly," from the theft of the trade secret.³⁷ The court may also order the forfeiture of "any of the person's [or organization's] property used . . . to commit or facilitate the commission [of the offense]."³⁸ With regard to the latter provision, the court may in its discretion take into consideration "the nature, scope, and proportionality of the use of the property in the offense."³⁹ The property in question is forfeited to the United States, rather than to the victim of the crime.⁴⁰ The legislative history of the EEA, however, suggests that

³⁵ This section provides:

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

³⁶ "Understanding the Economic Espionage Act of 1996" at 203.

³⁷ 18 U.S.C.A. § 1834(a)(1).

³⁸ 18 U.S.C.A. § 1834(a)(2).

³⁹ *Id.*

⁴⁰ *Id.*

victims may be able to seek restitution from the United States out of the forfeited proceeds.⁴¹

Section 1834 of the EEA provides that, with certain minor exceptions, the forfeiture of proceeds and instruments shall be governed under the laws relating to drug forfeitures. Those laws vest title to the seized property in the United States, and provides that the Attorney General shall dispose of those assets “by sale or any other commercially feasible means.”⁴² It has been suggested that this requirement may pose a problem to the owner of the trade secret because where the seized assets include a product embodying the trade secret, the sale by the government of this product could result in the further dissemination of the trade secret which, of course, is inconsistent with the victim’s interest in keeping the information secret.⁴³

Although such a reading of the statute is literally correct, it is extremely unlikely for it to ever be more than a theoretical issue: First, the property embodying the trade secret seized from the defendant is directly analogous to seized counterfeit goods such as computer CDs, T-shirts and watches.⁴⁴ In such instances, the government does not sell the counterfeit property to the highest bidder, but destroys the property, often in a manner designed to obtain maximum publicity and deterrence value, such as by publicly crushing the counterfeit items with a steamroller. Second, it is extremely unlikely and illogical that the government, having acted to preserve a trade secret, would then jeopardize this through the public sale of goods embodying the trade secret.⁴⁵

[f] Extraterritorial Application

Section 1837 governs the applicability of the EEA to conduct that occurs, in whole or in part, outside the United States. The scope of the EEA under § 1837 is extremely broad and is consistent with the goal of the EEA of reaching foreign espionage, much of which occurs outside the United States. For example, under this subsection, a foreign corporation that sells a product in the United States that embodies a stolen trade secret can be

⁴¹ 142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996) (statement of Sen. Nickles).

⁴² 21 U.S.C.A. § 853.

⁴³ “Understanding the Economic Espionage Act of 1996” at 202.

⁴⁴ *See, e.g.*, 18 U.S.C.A. § 2319A(c).

⁴⁵ Some people might argue that the illogic of the situation makes it likely that the government would act in that fashion.

prosecuted in the United States if the misappropriation occurred here. This is true regardless of where the product was manufactured. Significantly, the EEA also expressly applies to wholly foreign acts of economic espionage if the defendant is either a permanent resident alien of the United States or a U.S. corporation. Because of the broad reach of the EEA, foreign companies that do business in the United States or with American companies must become particularly sensitive to the scope of the EEA to avoid running afoul of its provisions.⁴⁶

Further, although the United States could exercise jurisdiction under § 1837(2) in a situation where a non-American company misappropriated a trade secret from another non-American company on the basis that an act in furtherance of the offense was committed in the United States, it is extremely unlikely that a United States Attorney's Office would agree to prosecute such a case because involvement in such an extraterritorial matter by a United States Attorney's Office would be a waste of scarce resources and could also lead to the United States' becoming involved in what is essentially an internal dispute in a foreign country.

[g] Construction With Other Laws

Section 1838 states that "[t]his chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal provided by United States Federal, State . . . or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5" (commonly known as the Freedom of Information Act). Thus the EEA does not block any possible existing remedies and could be charged in combination, in appropriate circumstances, with other existing federal criminal laws such as criminal copyright infringement.⁴⁷

[h] Department of Justice Oversight

In general, United States Attorney's Offices have almost absolute prosecutorial discretion in whether to open a criminal investigation and seek an indictment for an alleged violation of federal criminal law. Except in limited cases involving high profile crimes or national security matters, United States Attorney's Offices do not consult, and are not required to seek the

⁴⁶ For a further discussion of this issue, see "EEA Violations Could Trigger Criminal Sanctions," Hoken S. Sekei and Peter J. Toren, *The National Law Journal*, August 25, 1997 at B8.

⁴⁷ 18 U.S.C.A. § 2319.

approval of, the Attorney General or other Department of Justice officials in Washington. However, prior to the passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice will require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.⁴⁸

28 C.F.R. § 0.64.5 expressly implements this requirement and also provides that “[v]iolations of this regulation are appropriately sanctionable and will be reported by the Attorney General to the Senate and House Judiciary Committees. Responsibility for reviewing proposed charges under the EEA rests with the Computer Crime and Intellectual Property Section, Criminal Division, which will consult with the Internal Security Section, Criminal Division, in cases involving charges under 18 U.S.C.A. § 1831.” Congress imposed this notice requirement to try and prevent United States Attorney’s Offices from taking sides in purely business disputes.

[i] Potential Defenses

The EEA does not contain any reference to possible defenses. The legislative history of the EEA makes clear that parallel development or reverse engineering of the trade secret under certain circumstances could be a defense. Further, the legislative history also makes clear that an employee should be permitted to take his general skill and knowledge from one job to the next. The distinction between general knowledge that can be exploited and trade secret information that cannot be legally used by other than its rightful owner is very difficult to make. However, the importance of making this distinction in today’s high-tech economy in which employees change jobs with great frequency

⁴⁸ The legislative history contains no suggestion as to why Congress sought and obtained this promise from the Attorney General. It has been suggested, however, that Congress was concerned that: (1) a United States Attorney’s Office could make use of the EEA for political purposes, such as by threatening to prosecute, or agreeing not to prosecute, a corporation or powerful individual within its jurisdiction; or (2) a United States Attorney’s Office could have an effect on United States foreign policy by indicting, without the knowledge of anyone in Washington, a foreign government official. The latter reason is more persuasive since a United States Attorney’s Office could use almost any federal criminal law as part of a threatened indictment. Whereas, for example, if the United States Attorney’s office for North Dakota indicts a French government official without the knowledge of the Attorney General or the State Department, it could have an impact beyond the confines of the boundaries of North Dakota and could affect the relationship between the United States and France.

cannot be underestimated. It can mean the difference to a company between being investigated and prosecuted for theft of trade secrets under the EEA, and lawfully profiting from the general knowledge and skills brought to the company by a new employee. For this reason, parallel development, reverse engineering and general knowledge and skills will be discussed, in turn, as potential defenses to an EEA charge.

[j] Parallel Development

The legislative history of the EEA adopts the well-established, civil trade secret law precept that a person who develops a trade secret, unlike the holder of a patent, does not have an absolute monopoly on the information or data that comprises the trade secret.⁴⁹ Thus, the EEA “does not in any way prohibit companies, manufacturers, or inventors from using their skills, knowledge and experience to solve a problem or invent a product that they know someone else is also working on.”⁵⁰ In that respect, it is very important for companies to maintain accurate records showing in detail the steps taken to independently develop the trade secret. Thus, if faced with an allegation of theft, a company can document how it independently developed the trade secret.

[k] Reverse Engineering

Reverse engineering refers to the generally lawful practice of taking something apart to determine how it was made or manufactured.⁵¹ The legislative history of the EEA suggests that the focus of whether a trade secret was lawfully reverse engineered should be on “whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has ‘reverse engineered.’ If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent,

⁴⁹ 142 Cong. Rec. S12212 (Oct. 2, 1996), citing *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 490-91 (1974) (“If something is to be discovered at all very likely it will be discovered by more than one person Even were an inventor to keep his discovery completely to himself, something that neither the patent nor trade secret laws forbid, there is a high probability that it will be soon independently developed. If the invention, though still a trade secret, is put into public use, the competition is alerted to the existence of the inventor’s solution to the problem and may be encouraged to make an extra effort to independently find the solution . . .”).

⁵⁰ *Id.*

⁵¹ *See, e. g., Kewanee*, 416 U.S. at 476 (The law does not protect the owner of a trade secret from “discovery by fair and honest means, such as independent invention, accidental disclosure, or by so-called reverse engineering.”).

or this law, then that form of 'reverse engineering' should be fine."⁵²

It has been suggested that if this understanding of the scope of permissible reverse engineering under the EEA is adopted by the courts, it would have a chilling effect on the development of new technology.⁵³ In support of this claim, the authors cite the use of a decompiler to reverse engineer computer source code. Because the use of a decompiler almost always involves the making of a prohibited "copy" of the program, it is argued that such an act would be illegal under the EEA,⁵⁴ although it would not be actionable under civil law.⁵⁵ Although this interpretation of the EEA may be literally correct, it is extremely unlikely that a United States Attorney's Office would seek to prosecute, and that the Department of Justice would approve the criminal prosecution of, an individual who could not be held liable under civil trade secrets law. Further, such an understanding of the EEA is inconsistent with Congress's intent that the EEA is intended to be applied only "in flagrant and egregious cases of information theft."⁵⁶

[I] General Knowledge

The EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill or abilities. The legislative history makes clear that "[t]he government can not prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains by or during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior."⁵⁷ Thus, for example, employees who change jobs cannot be prosecuted under the EEA on the grounds that they were exposed to a trade secret while employed. This does not mean, however, that employees who leave a company to start their own companies can never be prosecuted under the EEA. Where the employees stole or without authorization appropriated a trade

⁵² *Id.*

⁵³ "Understanding the Economic Espionage Act of 1996" at 195.

⁵⁴ *Id.*

⁵⁵ *Id.* at 19.5-96 ("A computer programmer has the right to decompile a software program in certain circumstances under the USTA, copyright law, and the common law, without fear of civil liability.").

⁵⁶ 142 Cong. Rec. S12212 (Oct. 2, 1996) (Manager's statement).

⁵⁷ *Id.* at S12213.

secret from their employer, they may be prosecuted under § 1832, assuming, of course, that the other elements of the statute can also be satisfied. The First Circuit in *United States v. Martin*,⁵⁸ explained that the EEA “was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It was, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere.”

[m] Prosecutions Under the EEA

Although it is hard to generalize what type of misconduct the Department of Justice will approve as suitable for prosecution under the EEA, based on the prosecutions brought by the government to date, it appears unlikely that the government will prosecute run-of-the-mill theft of trade secret cases. This should offer some reassurance to those who were concerned when the EEA was enacted that the government might end up taking sides in purely business disputes or that the Act was solely intended to provide work for the FBI. Following is a description of the prosecutions that have been brought under the EEA to date:⁵⁹

1. *United States v. Worthing* (W.D. Pa.)—In the first prosecution brought under the EEA, Patrick Worthing was caught on tape offering to sell proprietary information he stole from Pittsburgh Plate Glass to an undercover FBI agent whom Worthing believed was working for PPG’s competitor and rival, Owens Corning. Patrick’s brother, Daniel, was also charged with assisting Patrick in exchange for \$100. Both defendants pleaded guilty. Patrick Worthing was sentenced to fifteen months in prison. Daniel Worthing received five years’ probation including six months of home detention.

2. *United States v. Hsu* (E.D. Pa.)—A grand jury indicted defendants Kai Lo Hsu and Chester Ho for conspiring to obtain and attempting to obtain trade secret information from Bristol-Myers relating to an anti-cancer drug known as Taxol.⁶⁰ The FBI arrested the defendants after a meeting with an undercover agent and a Bristol-Myers scientist, and after allegedly

⁵⁸ 228 F.3d 1 (1st Cir. 2000).

⁵⁹ See, e.g., Robert Dreyfus “Spy vs. No-Spy,” *The New Republic*, December 23, 1996.

⁶⁰ *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998).

reviewing actual Bristol-Myers documents relating to Taxol and bearing confidential markings.

3. *United States v. Yang* (N.D. Ohio)—On April 28, 1999, a jury convicted defendants P.Y. Yang, H.C. Yang and Four Pillars, Inc. of conspiracy to steal trade secrets and attempted theft of trade secrets from the Avery Dennison Corporation. The defendants had obtained the trade secrets from a senior engineer at Avery, Victor Lee, over the course of an eight year period beginning in 1989.⁶¹ Mr. Lee pleaded guilty to one count of wire fraud and cooperated with the government. The trial judge, despite evidence that the value of the purloined trade secrets was over \$10 million, sentenced both of the individual defendants to home detention. He fined the corporation the \$5 million maximum permitted by statute. The government is appealing the sentences imposed on the individual defendants.

4. *United States v. Steven Davis* (D. Mass.)—Steven Davis, who was an engineer at a company under contract to Gillette to assist in the development of the new Mach 3 shaving system pleaded guilty to sending confidential Gillette information relating to this shaving system to the Bic Corporation.⁶² Davis was sentenced to twenty-seven months in prison and ordered to pay \$1.2 million in restitution to Gillette.⁶³

5. *United States v. Trujillo-Cohen* (S. D. Tex.)—The defendant pleaded guilty to providing copies of certain proprietary software programs belonging to her former employer, Deloitte-Touche, to two subsequent employers. She also provided a “teaser” of one of the programs to another company in order to induce them to hire her as a consultant and to pay her a \$10,000 signing bonus. Trujillo-Cohen was sentenced to forty-eight months’ imprisonment and ordered to pay \$337,000 in restitution to Deloitte-Touche.

6. *United States v. Campbell* (N.D. Ga.)—The circulation manager for the Gwinnett Daily Post, Carroll Lee Campbell, Jr., pleaded guilty to offering to sell proprietary circulation information to the Atlanta Journal-Constitution for

⁶¹ For a description of the facts in this case, *United States v. Yang, et al.*, 74 F. Supp. 2d 724 (N.D. Ohio 1999).

⁶² *United States v. Steven Louis Davis*, No. 97-123 (M.D. Tenn.).

⁶³ The Boston Globe (April 30, 1998) at E1 6.

\$150,000.⁶⁴ Campbell was sentenced to three months' imprisonment and four months' home confinement.

7. *United States v. Fulton (W.D. Pa.)*—Defendant John Fulton pleaded guilty to attempting to purchase proprietary information belonging to his former employer, Joy Mining Machinery Company. Fulton was arrested and charged after the FBI monitored a telephone call in which Fulton offered to pay \$1,500 to a current Joy Mining employee for proprietary diagrams relating to coal mining equipment. Fulton is awaiting sentencing.

8. *United States v. Krumrei (D. Haw.)*—Krumrei, a Michigan attorney, was charged with violating the EEA after the FBI surveilled a meeting during which the defendant allegedly disclosed three trade secrets relating to a new confidential process for applying a Formica-like coating to laminate contacting surfaces owned by an Australian company. In an interview with the FBI, Krumrei denied having stolen the information, and claimed that he obtained it from publicly available information and information previously disclosed to him by his former employer, who had been hired by the Australian company to assist with the development of the confidential process. The Australian company has assured the government that Krumrei could have obtained the information only through theft, not from publicly available sources and it has a confidentiality agreement with Krumrei's former employer. The information is allegedly valued in the millions of dollars.

9. *United States v. Hallsted & Pringle (E.D. Tex.)*—Defendants Steve Hallsted and Brian Pringle pleaded guilty to violating the EEA for offering to sell prototypes of a new Intel computer central processing unit known as the "Slot II" to one of Intel's competitors, Cyrex, for \$75,000. Intel has estimated that the company would have lost up to \$10 million dollars if a rival corporation had obtained a Slot II CPU before its introduction into the retail market. Defendants are awaiting sentencing.

10. *United States v. Huang Dao Pei (D. N.J.)*—The United States Attorney's Office for the District of New Jersey indicted Huang Dao Pei, a former scientist at Roche Diagnostics, for allegedly trying to obtain information from a current Roche employee who was cooperating with the government and secretly recorded his meeting with the defendant. Huang allegedly told the Roche employee that he needed to obtain information about Roche's hepatitis C diagnostic testing kit so that his company,

⁶⁴

United States v. Campbell (N.D. Ga.).

LCC Enterprises, could develop a similar kit and sell it in China. No trial date has been set.

11. *United States v. Camp* (D. Me.)—On September 16, 1998, a federal grand jury in Maine returned an indictment charging Caryn Camp and Dr. Stephen R. Martin with ten counts of wire fraud, two counts of mail fraud, one count of conspiracy to steal trade secrets, one count of conspiracy to transport stolen goods, and one count of interstate transportation of stolen goods. The trade secrets related to confidential information belonging to Ms. Camp's then current employer Idexx Labs, a Maine Company that manufactures veterinary supplies. The government became involved after Camp accidentally sent to her supervisor an e-mail stating that she had mailed a large number of stolen documents to Martin. The e-mail stated that the shipment included two boxes containing seven binders' worth of trade materials and that "there's some really cool stuff coming through, you'll feel like a kid on Christmas Day!" In a follow-up message to Martin after she apparently realized her stupidity, Camp wrote "I just screwed up, I think the biggest screw-up of my life. And I can't stop shaking, I'm so scared." Camp pleaded guilty and agreed to testify at trial. At trial, the jury convicted Martin four counts of wire fraud, two counts of mail fraud and the conspiracy counts.⁶⁵

[n] The Criminal Referral Process

[i] Advantages/Disadvantages of Prosecution

The EEA can provide important benefits to a trade secret owner. First, prosecution demonstrates that a company will take whatever steps are necessary to protect its proprietary and confidential information. Second, prosecution is an extremely effective deterrent. Third, because the federal government pays all costs, a corporation can greatly reduce its legal expenses by not having to hire private lawyers to litigate its claims. Fourth, federal law provides that the victim of a crime may obtain full restitution for its losses, and a corporation may be entitled to financial remuneration without having to incur legal costs.⁶⁶

The advantages of criminal prosecution, however, must be weighed against potential risks. The most significant disadvantage of criminal prosecution for a victim is ceding control of the process to the federal government, which may or may not have the same interests. For example, a victim cannot force the government to

⁶⁵ See *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000).

⁶⁶ 18 U.S.C.A. § 3663.

dismiss charges against the defendant as a condition for reaching a civil settlement. Further, the existence of a criminal prosecution may cause a court to stay a parallel civil proceeding greatly slowing down the victim's recovery of damages. Finally, because a criminal defendant is generally entitled to broader discovery, the existence of a criminal prosecution may lead to the disclosure of records and confidential information that the victim would not have been required to disclose in the civil litigation.

When making the decision whether to refer a theft of trade secrets to the government for possible prosecution, it is also important to understand that for a variety of reasons most theft of trade secret cases are not suitable candidates for criminal prosecution. First, Congress did not intend for the EEA to replace civil trade secret litigation. Second, United States Attorney's Offices are very busy and handle a wide variety of cases, which often involve defendants who are accused of violent crimes that are considered far more serious than the theft of trade secrets. Scarce resources have forced many United States Attorney's Offices to set guidelines to determine whether to investigate and prosecute white-collar crime cases, including those involving intellectual property. Third, the higher standard of proof in criminal cases may mean that, while a victim might have a very strong civil case, the matter may still be unsuitable for criminal prosecution and therefore be declined by a United States Attorney.

While there is no single factor that is likely to determine whether a United States Attorney's Office will prosecute a defendant for the theft of trade secrets, the following discussion addresses some of the factors that a United States Attorney's Office will examine and weigh in evaluating a referral. It is intended therefore to aid a victim in evaluating whether to refer a matter to the government for possible prosecution, and to maximize the chances for a successful referral.

[iii] Factors Leading to Prosecution

In determining whether to take a particular case, the prosecutor will take into consideration the following factors:

(1) *The Adequacy of the Security Measures*

In order to establish that criminal prosecution is warranted, the victim must be able to demonstrate to the satisfaction of the United States Attorney's Office that it used "reasonable measures"

to protect the information in question.⁶⁷ The EEA requires that the extent of the victim's efforts to protect sensitive information be commensurate with the value of the trade secret. In the current competitive intelligence climate, the government will carefully scrutinize the adequacy of the victim's efforts to protect its trade secrets because the defendant, in turn, will closely examine these procedures at trial. In particular, in evaluating the merits of a referral for a violation of the EEA, a United States Attorney's Office will seek to answer the following questions:

- (a) Is there objective and independently verifiable evidence demonstrating that the information is a trade secret?
- (b) Was the information of a discrete nature that can be readily distinguished from less protected information?
- (c) Has the victim or any of its subcontractors or licensees ever intentionally or inadvertently disclosed the information?
- (d) How was the distribution of information limited by the victim, if at all?
- (e) Were nondisclosure agreements used to protect the information from outsiders?
- (f) What other steps, such as password-protected electronic storage, encrypted data, physical security, were taken to protect the information?

(2) *The Type of Information Misappropriated*

Although the EEA expressly covers all types of information within the definition of trade secrets, the government, for a variety of reasons, is more likely to prosecute a matter involving the theft of scientific or research information than a matter involving pure business information. First, scientific information is likely to be worth more than business information and thus is more likely to meet the financial thresholds established by most United States Attorney's Offices. Additionally, the economic value of business information is often difficult to quantify in a meaningful way and has a short shelf life. In other words, business information may be valueless at the time of trial, which greatly diminishes its perceived significance and the jury appeal of the case.

⁶⁷ 18 U.S.C.A. § 1839.

Second, the EEA specifically requires that the alleged trade secret be “related to or included in a product that is produced for or placed in interstate or foreign commerce.” As of yet, there is no reported decision interpreting the scope of this requirement, however, it is possible that many types of business information, such as corporate expansion and development plans, may not satisfy this element of the statute.

(3) *Evidence of Misappropriation and/or Consciousness of Guilt*

In general, the EEA makes it a crime to obtain a trade secret by almost any means, including copying.⁶⁸ The EEA even covers situations where the lawful owner retains the original copy of the trade secret and is not deprived of its use. However, physical evidence of misappropriation is usually necessary to establish the intent elements of the statute, i.e., that:

- (a) The defendant intended to convert a trade secret to the economic benefit of someone other than the owner;
- (b) The defendant intended or knew that the offense would injure the owner of the trade secret; and,
- (c) The defendant misappropriated the information knowingly.

Without any physical evidence of theft, proving these required intent elements may be extremely difficult. Thus the government will be extremely wary of investigating and prosecuting a defendant if there is little or no physical evidence of theft.

In order to overcome this reluctance of the government to prosecute cases where there is little or no physical evidence of theft, the victim must be able to point to other evidence that can be used to establish intent, such as admissions or statements found in any correspondence, or through patterns of behavior that demonstrate a consciousness of guilt. For example, is there evidence that the defendant behaved in an inappropriate manner or evinced an intent to hide transactions? Is there information, such as computer logs, that would provide evidence of an unauthorized intrusion into a victim’s network, or prove that certain files had been accessed and copied by the unauthorized user? Without the existence of such evidence, it is unlikely that the government will

⁶⁸ *Id.* §§ 1831(a)(2), 1832(a)(2).

seek to prosecute an individual who misappropriated the trade secret by hiding it in the recesses of his mind.

(4) *Cooperation of the Victim*

Although not legally required, in order for the government to get involved, the victim must be completely cooperative. Federal prosecutors have better things to do with their time than to attempt to prosecute a defendant where the victim does not fully support the prosecution. In other words, why should the government care if the victim doesn't? Moreover, unlike most other federal crimes, the information necessary to establish the elements of an EEA violation is usually in the victim's control, such as evidence of reasonable measures to keep the information secret, evidence about the nature and value of the stolen information, and access to the victim's documents and personnel. To put it simply, without the victim's full cooperation, the government will not prosecute.

(5) *Availability of Defenses*

Another important factor that the government will closely examine in deciding whether to open an investigation is whether there are potentially strong defenses available to the defendant. For example, the government will not want to become involved in a matter in which the defendant can creditably claim that he developed the trade secret independently or that the trade secret was reverse engineered. Other potential defenses also will be explored by the government, such as whether the trade secret was inadvertently disclosed in scientific journals or intentionally disclosed through, for example, the filing of a foreign patent application. The government will more closely examine the applicability of potential defenses in situations where there is little or no physical evidence of misappropriation.

(6) *Timing of the Referral*

In most instances, the government will view timely referrals with favor. As with any crime, prompt reporting increases the likelihood that relevant evidence will be located. In the theft of trade secret context, prompt reporting reduces the likely applicability of some relevant defenses, such as reverse engineering or parallel development. However, the possibility that a prompt referral will lead to criminal prosecution may be outweighed by the benefits of a thorough investigation.

The likelihood of acceptance of the case may increase dramatically if the victim thoroughly investigates the matter and is able to present a "beautifully wrapped" case file to the United States Attorney's Office for review. Such a ready-made case often can be very appealing to overworked federal investigators and prosecutors. Further, it demonstrates to the government that the victim is serious and will cooperate fully in the investigation and prosecution. Thus, victims who want to maximize their chances for a successful criminal referral, upon discovery of the theft, should contact experienced outside legal counsel to discuss whether the matter should be investigated privately or should be immediately reported to the government.

(7) *Value of the Misappropriated Information*

The EEA does not contain a jurisdictional monetary amount. However, most United States Attorney's Offices have established monetary thresholds in white-collar cases for investigation and prosecution. Thus, the monetary loss to the victim must be great enough to warrant criminal investigation and prosecution. This minimum threshold varies from office to office, but in some large districts, such as the Central District of California (Los Angeles) or the Southern District of New York (Manhattan) the loss to the victim must exceed \$100,000. Since there is often no legitimate market for trade secrets, establishing economic loss can be difficult.

Although it can be difficult for a victim to accurately establish the value of the trade secret and its financial loss, victims should attempt to do so as accurately as possible. Many experienced government investigators and prosecutors are highly suspicious, and rightly so, of unsubstantiated loss figures supplied by the victim. Therefore, victims should provide the government, as early as possible in the referral process, with documents or other evidence to permit the government to attempt to independently verify the extent of the loss. This is extremely important because independent estimates of significant loss usually weigh heavily in favor of investigation and prosecution.

(8) *Availability/Sufficiency of Civil Remedies*

Even if other factors strongly suggest that investigation and prosecution is warranted, a United States Attorney's Office may decline the matter because of the availability and adequacy of civil remedies. Although this factor alone should not in and of itself be determinative of whether to prosecute because a victim of a theft of the secret almost always has a civil remedy, the completeness of

the civil remedy will be carefully examined by a United States Attorney's Office.

In determining the completeness of the victim's civil remedy, the government can be expected to ask the following questions:

- (a) Is the defendant judgment proof?
- (b) Does the victim have the financial resources to pursue a civil remedy?
- (c) Is the defendant's conduct pervasive or far reaching?
- (d) Can the defendant be located without the assistance of law enforcement?
- (e) Are state trade secret laws inadequate?

If all these questions can be answered in the negative, it is extremely unlikely that the government will investigate and prosecute.

[o] Procedure

The procedure of making a referral to the government for the theft of trade secrets is identical to that for all criminal referrals to the federal government involving white collar crime. The first step is for the victim or its attorney to contact the local United States Attorney's Office or the FBI office. If the decision is made to first contact the United States Attorney's Office, the victim should seek to discuss the matter directly with the Assistant who has been designated the Computer and Telecommunications Coordinator or "CTC" for that Office. There is at least one CTC in every United States Attorney's Office and they have received specialized training from the Computer Crime and Intellectual Property Section in Washington in this area of the law among others.

Although the CTCs must follow the prosecutive guidelines of their respective office there is some flexibility and discretion in the system. It is more likely that a theft of trade secret referral made directly to an Assistant United States Attorney, who already understands the law and often has greater understanding of

recommend that it should be opened for investigation and prosecution. Further, from a human standpoint, because most CTCs are genuinely interested in this subject matter and often will end up prosecuting the case themselves, it is to the victim's

technical issues, will v

advantage to get them familiar with the matter as early in the referral process as possible.

Finally, if the victim believes that the United States Attorney's Office should not have declined the matter, the victim should consider discussing the matter with an attorney in the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, D.C. The Section's attorneys have considerable expertise in this area, and the Section has the resources to prosecute cases, including those that have been declined by a United States Attorney's Office.

[p] Avoiding or Reducing Corporate Criminal Exposure

There has been a lot of discussion since the passage of the EEA that corporations will be prosecuted under the EEA for activities that they routinely previously engaged in, such as collecting competitive intelligence. Although this is extremely unlikely to happen, corporations should examine their procedures on the handling of confidential information in order to avoid or reduce corporate criminal exposure should the unthinkable occur. Moreover, by enacting these basic procedures, corporations will reduce their civil liability exposure. In general, standards regarding contracting authority and rules for entering into nondisclosure agreements should be reviewed. Hiring and personnel practices should be investigated with the goal to avoid hiring employees who intend to use the trade secrets of their former employees. Procedures should be put into place to ensure that the intellectual property rights of others are respected.

The most important feature of any strategy for avoiding or mitigating corporate exposure under the EEA is a "compliance plan." In fact, the Federal Sentencing Guidelines, which must be followed by all federal courts, provide that an "organization"⁶⁹ can reduce its culpability by establishing and maintaining an effective program to prevent and detect violations of the law. Moreover, a good compliance plan also can aid in convincing a United States Attorney's Office and the Justice Department that prosecution of the corporation is not warranted because the corporation itself was victimized by a "rogue" employee.

⁶⁹ "Organization" as defined by the guidelines includes corporations, partnerships, associations, nonprofit organizations, pension funds, unions and unincorporated organizations.

The primary goal of a compliance plan is to actually prevent unauthorized secrets from becoming part of the company's knowledge base. Because a good compliance plan will by definition raise the level of awareness within the organization about the importance of intellectual property, it will also lead to the increased protection of a company's own intellectual property. Since the loss or disclosure of most corporate trade secrets is most often caused by accident or negligence, a compliance plan can be an extremely effective and cost efficient way to safeguard a company's own confidential information.

Other general goals of a successful compliance plan are to increase the likelihood of early discovery and avoid liability in civil litigation. Civil lawsuits for trade secret misappropriations are on the increase, especially in technology-related industries. Just as in the criminal context, the implementation of a compliance plan is not a shield against all civil lawsuits, but it does reduce their likelihood and potential liability.

The following is a description of the eight most important elements of a compliance plan as proscribed by the Federal Sentencing Guidelines.⁷⁰

(1) *Standards and Procedure*—The plan must include “standards and procedures to be followed” by all the employees of the organization.⁷¹ The standards should be specific enough to guide the employees in the exercise of their daily jobs. This part of the plan must also include such specific details as to the steps an employee must follow if a problem is identified, and the consequences for failing to comply.

(2) *Oversight*—The sentencing guidelines require that the plan be implemented by “high level personnel of the organization.”⁷² Thus, ultimate responsibility for the plan must lie with a management level person who has the authority to assure that the plan is followed. Furthermore, the President, CEO and Board of Directors should be kept regularly informed about the status of the plan.

(3) *Due Care in Delegation of Authority*—The plan must not give “discretionary authority to individuals whom the organization knew or should have known through due diligence to

⁷⁰ 18 U.S.C.A. § 8A1.2, comment (n.3)(k).

⁷¹ *Id.* at comment (n.3)(k)(1).

⁷² *Id.* at comment (n.3)(k)(2).

have a propensity to engage in illegal activities.”⁷³ Background checks and careful scrutiny of resumes and references are examples of necessary procedures in this area.

(4) *Communication and Training*—The compliance plan must include steps to communicate standards through training programs.⁷⁴ The plan should focus initially on new employees, but also must be ongoing to inform existing employees about new developments in this area.

(5) *Monitoring and Auditing*—The plan must include procedures to supervise the company’s operations to assure that violations are likely to be detected and reported within the organization.⁷⁵ The monitoring should be periodically audited to assess the plan’s effectiveness and to make any changes if needed.

(6) *Discipline*—The plan’s standards must be “consistently enforced through appropriate discretionary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense.”⁷⁶ The organization, therefore, must keep careful records that violators were subject to appropriate discipline.

(7) *Reporting*—After a violation has been detected, the organization must take “all reasonable steps to respond appropriately to the offense and to prevent further similar offenses.”⁷⁷

The sentencing guidelines also stress that the compliance plan should be tailored to fit the individual characteristics of the company. An effective compliance plan, therefore, must reflect the following factors: (a) size of the organization; (b) risks associated with the company’s business; (c) past history of security problems or trade secret thefts; and (d) any applicable industry of government standards related to government security.⁷⁸

⁷³ *Id.* at comment (n.3)(k)(4).

⁷⁴ *Id.* at comment (n.3)(k)(5).

⁷⁵ *Id.* at comment (n.3)(k)(5).

⁷⁶ *Id.* at comment (n.3)(k)(6).

⁷⁷ *Id.* at comment (n.3)(k)(7).

⁷⁸ *Id.* at comment (n.3)(k)(7)(i-iii).

CITE: [The White House, Office of the Press Secretary. (Jan. 18, 2001). President Clinton Names Eighteen Members to the National Infrastructure Assurance Council [Press release]. Retrieved from National Archives and Records Administration <<http://clinton6.nara.gov/2001/01/2001-01-18-members-named-to-national-infrastructure-assurance-council.html>>.]

[View Header](#)

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release January 18, 2001

PRESIDENT CLINTON NAMES EIGHTEEN MEMBERS TO THE NATIONAL INFRASTRUCTURE ASSURANCE COUNCIL

President Clinton today announced his intent to appoint eighteen members to the National Infrastructure Assurance Council:

Mr. Alfred R. Berkeley, III, of Baltimore, Maryland, is the President of the Nasdaq Stock Market, Inc. Prior to joining Nasdaq, he was a Managing Director and Senior Banker in the Corporate Finance Department of Alex. Brown & Sons. Mr. Berkeley received a B.A. from the University of Virginia and an M.B.A. from the University of Pennsylvania.

Admiral Paul E. Busick, Jr., of Kinston, North Carolina, is the President and Executive Director of North Carolina's Global TransPark Authority. From 1996 to 1998, he served with the National Security Council as a Special Assistant to the President and Senior Director for Gulf War Illnesses. From 1993 to 1996, he served as Director of the Office of Intelligence and Security at the Department of Transportation and as the Secretary of Transportation's National Security Advisor. Admiral Busick received a B.S. from the United States Coast Guard Academy and an M.S. from Purdue University.

Mr. David H. Langstaff, of Comus, Maryland, currently serves as President, CEO, and Vice Chairman of the Board of Directors of Veridian Corporation. Veridian is a knowledge systems company that provides information-based solutions in the fields of global security, cyber assurance and safety. Mr. Langstaff served as Executive Vice-President and Chief Operating/Financial Officer of Space Industries International, Inc. and Calspan SRL Corporation. Mr. Langstaff received a B.A. and an M.B.A. from Harvard University.

Mr. Robert G. Liberatore, of the District of Columbia, has served as Senior Vice President of External Affairs and Public Policy for Daimler Chrysler Corporation since 1998. Prior to the Daimler Chrysler merger, he was Vice President of Washington Affairs for Chrysler Corporation. Mr. Liberatore joined Chrysler Corporation in 1985 after working on Capitol Hill for ten years, including four years as Staff Director for Senator Robert C. Byrd. Mr. Liberatore received a B.S. from Georgetown University.

Mr. Harris N. Miller, of Arlington, Virginia, is the President of the Information Technology Association of America (ITAA), the largest and oldest information technology trade association. Prior to joining ITAA, he was the President of the World Information Technology and Services Alliance. Mr. Miller received a B.A. from the University of Pittsburgh and an M.A. from Yale University.

Mr. Alan Paller, of Bethesda, Maryland, is Director of Research of the SANS Institute, a cooperative research organization that delivers graduate-level education to information system professionals. He is also the co-founder of the CIO Institute. Mr. Paller received degrees from Cornell University and the Massachusetts Institute of Technology.

Governor Gary Locke, of Seattle, Washington, was elected Washington State's 21st governor on November 5, 1996, making him the first Chinese-American governor in U.S. history. As governor, he has worked to make Washington public schools the best in the nation, promote jobs and economic development in rural and urban areas, and fight juvenile crime. He received a B.A. in Political Science from Yale University and a J.D. from Boston University.

Mr. Raymond L. Ocampo, of Hillsborough, California, is Chairman of the Board of the Berkeley Center for Law and Technology and serves on the board of directors of PMI Group, Inc. He retired in November 1996 as Senior Vice President, General Counsel and Secretary at Oracle Corporation, the world's second largest software company. Mr. Ocampo received a bachelor's degree from UCLA and a J.D. from the University of California.

Lieutenant General Peter Albert Kind, of Red Wing, Minnesota, directed the National Y2K Information Coordination Center. He also directed the Defense Advanced Research Projects Agency Information Science and Technology Study Group, the Department of Defense Technical Area Review and Assessment panels and the National Infrastructure Assurance Council. He received an B.S. from the University of Wisconsin and a M.B.A from Harvard University.

Dr. Philip Chase Bobbitt, of Austin, Texas, currently holds the University of Texas A.W. Walker Centennial Chair in Law. He is the author of several articles and four books concerning Constitutional and Democratic theory. Dr. Bobbitt served from 1997 to 1999 as Director of Intelligence on the President's National Security Council. He received a B.A. from Princeton University, a J.D. from Yale Law School and a Ph.D. from Oxford.

Mayor Wellington E. Webb, of Denver, Colorado, was elected Mayor of Denver, Colorado, on May 4, 1999. He currently serves as the President of the United States Conference of Mayors, the Vice President of the National Conference of Black Mayors, and the Vice President of the National Conference of Democratic Mayors. Mayor Webb received a B.A. in Sociology from the Colorado State College at Greeley and an M.A. from Northern Colorado University.

Mr. William H. Gates, of Seattle, Washington, is Co-founder, Chairman and Chief Software Architect of Microsoft Corporation, the worldwide leader in software, services and internet technologies for personal and business computing. In 1999, Gates wrote *Business @ the Speed of Thought*, a book that demonstrates how computer technology can solve business problems in fundamentally new ways. Mr. Gates attended Harvard University.

Mr. Richard K. Davidson, of Allen, Kansas is Chairman and CEO of the Union Pacific Corporation. He began his career with the railroad services in 1960, while attending college. Mr. Davidson received a B.A. from Washburn University and has completed the program for Management Development at Harvard University.

Mr. James Phillip Chandler, of the District of Columbia, is head of the National Intellectual Property Law Institute. He is Emeritus Professor of Law at the George Washington University and Chairman and President of the Chandler Law Firm Chartered. Mr. Chandler received his B.A. from the University of California, Berkeley, a J.D. from the University of California, Davis, and a LL.M. from Harvard University.

Mr. Erle Nye, of Forth Worth, Texas, is Chairman and Chief Executive of Texas Utilites (TU) Company. He is also Chairman of the Board and Chief Executive of TU Electric, TU Fuel Company, TU Mining Company, TU Services, TU Properties Inc., and TU Communications, Inc. Mr. Nye holds a B.S. in Electrical Engineering from Texas A&M University and a J.D. from Southern Methodist University.

Mr. Charles R. Stuckey, Jr., of Carlisle, Massachusetts, is Chairman of RSA Security, Inc. He joined RSA Security in January 1987, bringing to the firm over 20 years of experience in general management and high technology sales. Mr. Stuckey also serves on the Board of Directors of the Massachusetts Telecommunications Council and MatrixOne. Mr. Stuckey received a B.A. in Mechanical Engineering from Ohio University.

Ms. Judith Rodin, of Philadelphia, Pennsylvania, began her current duties as the President of the University of Pennsylvania in 1993. She serves on the boards of AETNA, Inc., the AMR Corporation, Electronic Data Systems, the Brookings Institution, Catalyst, and the Greater Philadelphia First Corporation. She currently serves on the President's Committee of Advisors on Science and Technology. She received a B.A. with honors from the University of Pennsylvania.

Mr. Jack Quinn, of Chevy Chase, Maryland, is co-chairman of Quinn Gillespie & Associates, LLC, a strategic consulting company he formed in January 2000. Previously, Mr. Quinn was a partner in the Washington, D.C. law firm of Arnold & Porter. In addition, he also served as Counsel to the President from November 1995 to 1997 and then served as Vice President Gore's Chief of Staff and Counselor. Mr. Quinn holds both a B.A. and J.D. from Georgetown University.

Mr. Robin Hernreich, of Edward, Colorado, is currently the President of Remonov & Company, Inc., a private investment company. He was the past Chairman of Sigma Broadcasting Company, which controlled a number of radio and television stations. Mr. Hernreich was also the owner of Sigma Communications, a cellular telephone company. Mr. Hernreich received a B.A. and an M.B.A. from Washington University in St. Louis.

Mr. Arthur Levitt, Jr., of Brooklyn, New York is the current Chair of the Securities Exchange Commission, where he has served since July 1993. As Chair he has overseen the securities markets when they have reached new and unprecedented highs. He is a distinguished and respected figure in the area of finance and public service. He served as Chairman of the American Stock Exchange for eleven years, leaving in 1989 to devote his time to a publishing venture, including ownership of the newspaper Roll Call. Mr. Levitt received a B.A. phi beta kappa from Williams College.

Mr. Lawrence P. LaRocco, of Arlington, Virginia, is the Chairman of LaRocco and Associates,

Inc., a government relations and public affairs consulting firm. Mr. LaRocco is a former Member of the U.S. House of Representatives. From 1991-1995, he represented the State of Idaho, First District,. While in Congress, he served on the Banking, Finance and Urban Affairs and the Natural Resources Committees. After leaving Congress, Mr. LaRocco served as a Managing Director at the American Bankers Association for five years. He received a B.A. from the University of Portland and an M.S. from Boston University.

The National Infrastructure Assurance Council (NIAC) was established by Executive Order 13010 issued on July 14, 1999. NIAC is charged with enhancing the partnership of the public and private sectors to address threats to the Nation's critical infrastructure. Members of NIAC will work to propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems. NIAC will also monitor the development of Private Sector Information Sharing and Analysis Centers (PSISACs); and provide recommendations to the National Security Council and the National Economic Council on how these organizations can best foster improved cooperation among the PSISACs, the National Infrastructure Protection Center (NIPC), and other federal entities.

30-30-30

Date: Fri, 19 Jan 2001 13:35 -0500

From: The White House <Publications-Admin@PUB.PUB.WHITEHOUSE.GOV> To: White-House-Publications@pub.pub.whitehouse.gov Subject: 2001-01-18 Members Named to National Infrastructure Assurance Council Keywords: Appointment, California, Colorado, Crime, Defense,

District-Of-Columbia, Economy, Education, Environment,
Executive-Act, Foreign, Government, Healthcare, Idaho,
Information-Policy, Infrastructure, International-Economy,
International-Security, Kansas, Maryland, Massachusetts,
Mid-Atlantic-Region, Midwest-Region, Minnesota,
Monetary-Policy, Mountain-States-Region, New-England-Region,
New-York, North-Carolina, Ohio, Pennsylvania, Personnel,
Plains-States-Region, Security, Social, South-Region, Texas,
Transportation, Urban, Virginia, Washington, West-Region,
Wisconsin

Message-Id: <20010119183537.1.MAIL-SERVER@pub1.pub.whitehouse.gov>

Document-ID: pdi://oma.eop.gov.us/2001/1/19/20.text.1

CITE: [The White House, Office of the Press Secretary. (Jan. 18, 2001). President Clinton Names Eighteen Members to the National Infrastructure Assurance Council [Press release]. Retrieved from National Archives and Records Administration <<http://clinton6.nara.gov/2001/01/2001-01-18-members-named-to-national-infrastructure-assurance-council.html>>.]