Foreign Denial and Deception Committee
George Bush Center for Intelligence, [redacted]
Washington, D.C. 20505

(b) (3)
(b) (5)

FDDC 02/005
24 April 2002

MEMORANDUM FOR: Department of Justice Interagency Task Force on Unauthorized Disclosures

VIA: [redacted] Office of General Counsel

FROM: [redacted] Vice Chairman, FDDC

SUBJECT: Personal Views on the Inadequacy of Existing Laws Concerning Unauthorized Disclosures, and Recommendations for New Ones

REFERENCE: *Leaks: How Unauthorized Media Disclosures of US Classified Intelligence Damage Sources and Methods*

This note is intended to supplement the recent paper produced by the Foreign Denial and Deception Committee on leaks. It aims to address implications for legal reforms implied by the findings of that study. The thesis is straightforward: New laws addressing leaks of classified intelligence are urgently needed.

There is a lot of classified information in the press these days, but this note, like the paper, is only concerned with classified *intelligence* information. Even more narrowly, its focus is confined to intelligence *sources and methods*, namely, *how* intelligence is secretly collected and analyzed.

Lessons From the Past: Doing business-as-usual is a prescription for failure

Do we need new laws to address the issue of unauthorized disclosures of classified intelligence information in the media? Answering this question requires some appreciation for the past experience of consistent failure. To date, the most authoritative study addressing unauthorized disclosures is the 1982 "Willard Report" (after its chairman Richard K. Willard, Deputy Assistant Attorney General, *Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information*, 31 March, 1982, prepared for the President). It concludes:

> "In summary, past experience with leak investigations has been largely unsuccessful and uniformly frustrating for all concerned . . . **This whole system has been so ineffectual as to perpetuate the notion that the government can do nothing to stop the leaks."** (Emphasis added).

The recommendations of the Willard Report for legal correctives resulted in proposed legislation in 1984. Although supported by OMB and the Administration, the Intelligence Community later withdrew the recommended draft legislation due to a perceived lack of support.

Twelve years later, responding to a request from the Assistant to the President for National Security Affairs, the National Counterintelligence Policy Board completed another study and reported no discernible change. (*Report to the NSC on Unauthorized Media Leak Disclosures*, March 1996). The report explained the continuing failure as a result of two key factors:

- **"A lack of political will to deal firmly and consistently with unauthorized executive branch and Congressional leakers.** Unsuccessful government efforts to prevent unauthorized disclosures were attributed largely to a lack of political support.

- **The use of unauthorized disclosures as a vehicle to influence policy.** [Citing the 1987 Tower Commission Iran/Contra report]: 'Selective leaking has evolved to the point that it is a principal means of waging bureaucratic warfare and a primary tool in the process of policy formulation and development in Washington'." (Emphasis in the original)

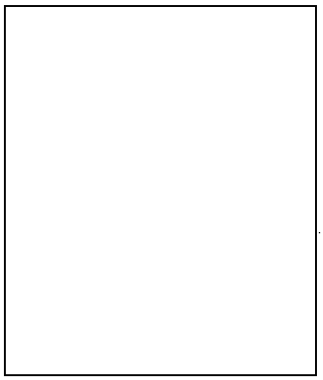
Given the palpable history of failure in protecting classified intelligence information from press disclosures—and given their epidemic proportions and the deleterious consequences they wreak in countermeasures to US collection effectiveness—it is fair to question whether past failed approaches will work today.

There has never been a general criminal penalty for the unauthorized disclosure of classified intelligence information to the press. Although intelligence leaks can technically be prosecuted under espionage statutes (18 USC 793 and 798), only a single case ever has (*US v. Morison*, 1988). Given that literally thousands of press leaks have occurred in recent years—many serious and virtually all without penalty—it is clear that *current laws do not provide an effective deterrent to leakers* or to journalists and their media outlets that knowingly publish classified intelligence.

A new approach—breaking from the failed past. If current trends in unauthorized disclosures are not reversed, such leaks will continue to compromise key sources and methods, and thereby seriously constrain US intelligence capabilities for the present and the future. Since so much now depends on a viable approach to the legal issues that have hamstrung past actions to address this debilitating problem, we need to understand some myths that have impeded past actions.

Popular Legal Myths about Unauthorized Disclosures of Intelligence

1. <u>The current laws are adequate</u>. Despite countless—literally thousands—of intelligence leaks in recent years, only a single violator (Morison, 1988) has ever been prosecuted. Willard's harsh judgment in 1982 that "the whole system is so ineffectual as to perpetuate the notion that the government can do nothing to stop leaks" is even more true today than when he wrote it. Morison notwithstanding, the 20 intervening years have seen neither a discernible abatement in



leaks, nor an improvement in governmental enforcement on this issue. If anything, the problem is getting worse.

Why is this the case? The obvious answer is that *the laws are only marginally applicable to leaks, and, as a practical matter, unenforceable in this application.* The statute under which Morison was prosecuted (18 USC 793) applies directly to espionage, but presents a real stretch for press leaks; and Morison *sold* the information to *Jane's Defence Weekly.* All agree that the government has always lacked the investigative ability to identify government leakers—and, as the National Counterintelligence Policy Board Study notes, also lacks the political will to bring any case forward. Such a case risks media cries of "chilling effect" on press discussions, and perhaps would even engender fear among federal employees. However, for press leaks, *these laws are irrelevant.* Defenders of the legal status quo need to explain the chasm between damaging leaks and the crippling lack of enforcement—and how present laws can successfully address this issue now when they never have before. I think they cannot even make a plausible argument in the face of the evidence at hand.

The lack of enforcement is itself the best indicator of the deficiencies in the law. Current law provides no appreciable deterrent to leakers or to their press publicists. Some journalists even demonstrate contempt for the law, and mock the government's inability to control leaks:

> "We believe in stories that make you say 'holy shit' when you read them, said Bill Gertz of *The Washington Times*, in a flattering profile of him that appeared in the conservative *Weekly Standard* . . . . Over the past couple of years, Mr. Gertz has written more stories based on classified government documents than you can shake a stick at, infuriating Clinton Administration officials and making a mockery of official classification policy." (Steven Aftergood, in *Secrecy in Government Bulletin*, No. 64, Jan., 1997, p. 1).

Mockery is correct. Journalists who traffic in classified information can proceed with high confidence that they can publish this information at will, and do so without penalty; and their government suppliers seem not to be deterred either. Laws that invite mockery because they are so ineffectual have lost whatever usefulness they might have had. Worse, they are positively counterproductive: They leave the impression of their adequacy *while keeping government legally paralyzed* to stem the hemorrhage of classified sources and methods appearing with alarming frequency in the US media.

2. Leaks really don't do much harm. The genealogy of this view traces to the publication of the Pentagon Papers. After much government carping about all the damage that those Top Secret revelations in the press would do to US national security, few today would claim that any damage was done at all. And certainly none to intelligence sources and methods. This view is given even greater credence by another popular myth that the government over-classifies everything, and classifies way too much. This seduction has become a creed among anti-secrecy proponents such as the National Security Archive and Federation of American Scientists. Publicly, this view is accepted uncritically, and never contested. Nor refuted. In fact, as the recent FDDC classified study of media leaks has convincingly shown, leaks *do* cause a great deal

of harm to intelligence effectiveness against priority issues including terrorism. But intelligence professionals also appreciate, and are much frustrated by, the fact that the best arguments for stopping intelligence leaks simply cannot be made in the press or in public forums, because of the paradoxical need to discuss—but protect—classified information.

3. Intelligence is adequately protected as "national defense information." This myth highlights the added legal difficulties of showing that intelligence sources and methods need also to be proven as "national defense" information to warrant protection under 18 USC 793, 798, and related laws. In truth, intelligence may or may not be so defined, but often, intelligence issues do not pertain directly to the national defense, and the added legal burden of meeting this defense requirement imposes still another pointless obstacle to legal remedies. Presently, the burden of proof is on the government to show that intelligence information relates directly to national defense, and further, that the person compromising it knew beforehand that its disclosure could harm the national defense. This burden is too high and off the mark. *What intelligence information needs is a separate, discrete, legal identification, independently of national defense.* This would create a legally-protected category of intelligence information that does not now exist. Other categories that *are* afforded effective protection include information on banking, crop estimates, taxes, and consumer credit. Surely intelligence sources and methods deserve as much. Sources and methods of intelligence collection are intrinsically important to the Nation's security, and intrinsically worthy of separate statutory protection. In removing impediments, this distinction would thus provide a major step forward in making enforcement—investigation and punishment—easier.

4. Public trials for secret issues are necessary. This bedeviling limitation has hamstrung the government in prosecuting espionage cases—and serves as a major inhibitor even in cases of unauthorized disclosures in the media. (It also provides a compelling rationale for military tribunals for terrorist cases involving foreign nationals). While the Classified Information Procedures Act (CIPA) affords good protection in pre-trial protection and "in camera" procedures, the perennial risk of exposing sensitive information in open court proceedings often deters the government from taking action. For example, an investigation of a major disclosure of highly classified information about sensitive collection activities might never be started—or could soon be halted—due to acute worries over further revelations about sources and methods. The reason? Intelligence agencies justifiably fear additional exposures of even more sensitive information in legal proceedings that would follow. As a result, significant leaks investigations always face the risk of being aborted after start-up, or are not started at all. This extraordinary Catch-22 is that *the greater the sensitivity—and intrinsic importance to national security—of the information compromised in the media, the greater the incentive for governmental inaction.* Poor laws that cannot adequately safeguard classified intelligence information in judicial proceedings *guarantee* continued governmental inaction—and continued media compromises of uniquely valuable sources and methods without penalty.

5. Journalists have every right to publish classified information. I do not understand how this myth got started, and it certainly doesn't apply to all journalists. But it applies to some. Unhappily, professional journalists must count within their ranks a few colleagues who traffic

heavily in classified intelligence—high volume, and often highly classified. When this minority of journalists arrogate to themselves the presumptive right to publish classified information in US newspapers and books, and on the Internet, it is fair to ask where they got this right. US classified information is produced by fully lawful procedures in the Executive Branch, and is subject to oversight by the Legislative Branch. No authorization to overturn this system extends to the Fourth Estate. But some journalists presume this "right" and exercise it presumptively on behalf of the American people—much to the detriment of the population they claim to serve when intelligence capabilities are weakened as a result.

These journalists either assume that existing law doesn't apply to them, or if it does that it won't be enforced, or that they are not breaking any laws at all. A few arrogant journalists—whose incomes and careers benefit from exploiting classified intelligence for profit—treat legally-classified intelligence as if it didn't deserve any protection at all. But their unquestioned legal right to do this has yet to be established in law. In practice, their actions subvert lawful regulations that fully intend to protect the intelligence they compromise in the press. In publishing classified intelligence, no journalist can convincingly claim a constitutional right to do so. Any journalist's "right" to publish information should not extend to classified information. But this legal argument remains to be made or adjudicated.

6. First Amendment protections prevent more restrictive legislation. For the most part, this is a canard. Identifying and punishing government leakers should not invite constitutional apprehensions. Leaking classified intelligence is no one's legal right, and publishing it in the press has not been demonstrated as the media's constitutionally-protected right either.

Still, the inherent tension between First Amendment rights and the government's interest in protecting national security is dynamic, and may never be solved "once and for all." But the current balance so favors First Amendment rights that legitimate national security interests are often superseded. This seems certainly the case with unauthorized media disclosures that compromise intelligence effectiveness. Here we should entertain redressing a potential legal imbalance by reconsidering a time-tested democratic principle enunciated by the preeminent philosopher of liberty, John Stuart Mill:

> **"... the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others."** *On Liberty* (1859).

Under the "harm principle"—for example, yelling "FIRE!" in a theater when there is none—a variety of exceptions to free speech are well established in American law such as obscenity, defamation, breach of peace, "fighting words," and sedition. To this list *we should add the compromise of US intelligence sources and methods required in the service of the Nation's security.* Government leakers with authorized access to the classified information they pass to journalists, and—certainly in *egregious* cases, also the journalists who traffic in classified intelligence—should be legally accountable for the sources and methods they expose that will

help foreign adversaries degrade the effectiveness of US intelligence, and thereby, further jeopardize US national security. By "egregious" I mean:

- When a covert intelligence officer or a foreign agent's identity is compromised in the media, thus risking exposure that may end in imprisonment or death.

- When multiple sources of fragile collection, including technical sensors, are compromised in the media, thereby incurring reduced effectiveness—for example, against priority targets such as Usama Bin Ladin or al-Qai'da—enfeebling analysis or warning through weakened collection.

- When extremely sensitive, highly classified, and costly collection programs are compromised in the media, resulting in foreign countermeasures that significantly reduce the program's cost-effectiveness.

- When unauthorized disclosures have so impaired intelligence on key national issues such as terrorism or proliferation of weapons of mass destruction that US policymakers are deprived of valuable information—including intelligence warning—not otherwise available, but essential to sound decisions and policies affecting US national security.

Attributes of a Good Law

The scope and seriousness of the intelligence leaks problem argue strongly for urgent attention to new law that can successfully stem the hemorrhage of classified intelligence that regularly appears in the media. *We need a specific statute that will deter leaks, and that will punish those who compromise classified intelligence that helps foreign adversaries defeat US sources and methods*. What attributes should such a law have? It should:

- Unambiguously criminalize unauthorized disclosures of classified intelligence information.

- Hold government leakers accountable for providing classified intelligence to persons who are not authorized access to that information.

- Define intelligence information—and specifically sources and methods—distinctly from defense information, creating a protected category of information less vulnerable to exposure under First Amendment rights.

- Provide better protection to sensitive and classified intelligence information in court trials and other judicial proceedings than is presently afforded through CIPA.

Should journalists have accountability? Much or all of the above attributes can be accomplished without inviting serious debate over First Amendment issues. More controversially, such a law would *also* hold uncleared publicists—i.e., journalists, writers,

publishing companies, media networks, and websites who traffic in classified information—accountable for damaging disclosures. Specifically, media *should* be held responsible for providing mass publicity to significant intelligence information they know to be classified, and whose exposure reduces US intelligence effectiveness by damaging sources and methods.

Present law already establishes such liability for media representatives who compromise the covered identities of US intelligence officers and agents (50 USC 421-426—but only as a *pattern* of activities, not for a compromise that could or does lead to the imprisonment or death of an agent caused by a single article); and also for compromises of SIGINT information (18 USC 798). Under these statutes—which have *never* been enforced against cases of unauthorized disclosures—compromises of imagery and other technical intelligence are not covered. And no generalized provision exists that will impose penalties for the publication of intelligence information that leads to foreign countermeasures that degrade, neutralize, or deceive US sources and methods of sensitive intelligence collection programs.

Consequences of inaction. Unless comprehensive measures are taken to identify and hold leakers accountable for the significant, often irreversible, damage they inflict on vital US intelligence capabilities, and, by implication, the degraded support such weakened intelligence offers to policymakers and warfighters, the damage will continue unabated. Conceivably, without some legally effective corrective action, the situation could even worsen. Under this scenario:

- Policymakers, warfighters, and military planners should expect that their *intelligence on significant national security issues will be less accurate, complete, or timely* than it would be without foreign countermeasures made possible by unauthorized disclosures.

- American citizens should expect that timely *warning of surprise attacks against the United States by terrorists or other hostile adversaries will be degraded* because key collection activities have been rendered less effective through unbridled leaks.

- US taxpayers should expect that their *multi-billion dollar collection programs will be less cost-effective* than they would otherwise be if foreign adversaries were not learning how to neutralize such programs through extensive classified information readily available in open sources.

The alternative is better intelligence capabilities for the United States. This can result from no added costs by merely better protecting the sources and methods we now have and those that are in the pipeline. Stemming press leaks will afford significantly better protection. Better laws—and enforcement of these laws—will make this possible. Present laws preclude improvement.