F.A.S. PUBLIC INTEREST REPORT

Journal of the Federation of American Scientists (FAS)

SECRECY REFORM

Volume 46, No. 4

July/August 1993

UNRAVELING THE TRIPLE HELIX OF GOVERNMENT SECRECY

In the post-Cold War period, after more than four decades of expansion, America's overblown and arthritic system for classifying secrets cries out for a complete revamping. The Clinton Administration has established a classification reform task force, but for reasons amply documented in this newsletter by FAS staffer Steven Aftergood, there is reason to doubt the task force's eventual efficacy.

Revamping the classification system will require more than task forces, "blue-ribbon" reports and idealistic rhetoric. It will have to confront, with credible processes, the triple-stranded helix of intertwined driving forces that produced the present excess: the urge to keep secrets, the well documented tendency of the bureaucracy to turn prudence into excess, and the relatively recent executive branch use of the secrecy system to enhance its power over Congress.

Thus, to untangle the helix, one must start from the top with the executive branch's blind-siding of Congress with "black budget" projects so highly classified that they are known, at most, to a handful of Congressmen—until, of course, they have reached a point of no return.

The Clinton Administration must involve the uniquely powerful constituency for reform at issue, the Congress. It should set in process an inter-branch committee of legislators and executive branch officials to determine mutually acceptable, and extremely limited, ground rules under which such super secrecy would be acceptable—and then embody the conclusions in legislation. If Congress will not fight for access to secrets denied it for political reasons, no administration will reform itself.

Next, the bureaucratic tendencies. One must cope with more than just the mindless application of rules that produced, last year, more than six million classification actions. There are, also, agency differentiated classification systems which require overburdened industrial firms to follow different procedures when dealing with different agencies in logging the documents in and out, transporting them, accounting for them, etc.—all ultimately at taxpayer expense.

Past efforts at reform suggest strongly that only a single, well-trained analyst, in the tradition of Robert McNamara, can make the myriad tradeoffs and judgments necessary to reverse the accretion of decades of bureaucratically induced complexity. In sum, perhaps only an intellectual Samurai, lopping off vestigial rules and knocking heads together, can roll back a bureaucracy.

Accordingly, at some stage, the Clinton Administration task force and the President's senior advisers should seek a distinguished analyst to complete their work and/or implement their main ideas. One advantage of this "single-mind" strategy is that it produces a personality that can testify in support of the reforms and explain them to Congress and the Executive Branch. (The advantages of this approach are expanded upon below on page 4.)

But the root strand of the triple helix of intertwined secrecy is the original, natural desire to keep secrets from enemies. Today, the enemy has shifted from a specific threat posed by a high-tech, developed country to the general threat of weapons proliferation to the Third World. But keeping general weapons technology from low-tech adversaries—who know so little that almost anything helps them—is not going to be easy. We may have to contain our impulse to classify the unclassifiable.

Perhaps a useful process here would be the Administration creation of an A-team, B-team enterprise. One team would survey the world literature and world industrial sources to show that the "secrets" involved could be secured by the Third World forces. The other would try to design methods of containing such secrets so as to help both teams determine a "waterline" below which secrecy was impossible or counterproductive.

The new Administration will find some constituencies already in place to support such initiatives. Congress itself ought to be weary of projects whose existence is officially denied, since such secrecy effectively denies Congress serious oversight.

Industry, as well as government, wants to be freed from unnecessary costs of secrecy, and some unusual official complaints, noted herein, show that in the post-Cold War era, it is not only liberal reformers who oppose the present system. Finally, there is a well-developed public interest sector devoted to asserting the public's right to know.

(continued on next page)

In sum, the need to overcome excessive secrecy represents a consensual issue that the Clinton Administration might find desirable for openers. ■

—Jeremy J. Stone

CLINTON REFORM DIRECTIVE

On April 26 President Clinton issued a directive that establishes a classification reform process, which is to culminate in the preparation of a new executive order on the classification of national security information. Excerpts from the sanitized version of the April 26 directive are presented below.

PRESIDENTIAL REVIEW DIRECTIVE 29

Subject: National Security Information

Background:

With the end of the Cold War, we should re-evaluate our security classification and safeguarding systems, as articulated in Executive Order 12356, to ensure that they are in line with the reality of the current, rather than the past, threat potential.

Objective:

The objective of this tasking is to review Executive Order 12356 and other directives relating to protection of national security information with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post Cold War period.

Questions:

The following sets forth the questions that should be addressed during this review. The resulting answers should serve as the basis for the drafting of the new proposed executive order which will be submitted upon completion of the review. ***(Editor's note: Questions posed in the Directive are repeated in this issue of the newsletter.)***

Implementation:

This review should be conducted under the chairmanship of the Director of the Information Security Oversight Office (ISOO) in coordination with the National Advisory Group for Security Countermeasures. Representatives of the agencies which comprise the NAG/SCM shall be included in the task force. It is further directed that this review be coordinated with the joint DCI-Secretary of Defense Security Commission.

The Chairman of the task force shall report to me through the NSC staff, Office of Intelligence Programs. The review should be completed no later than November 30, 1993, at which time a draft executive order superseding E.O. 12356 should be submitted for formal coordination. ■

FAS

Chairman: *Robert M. Solow
Vice Chairman: Richard L. Garwin
President: Jeremy J. Stone
Secretary: Ann Druyan
Treasurer: Carl Kaysen

The Federation of American Scientists (FAS), founded October 31, 1945 as the Federation of Atomic Scientists (FAS) is the oldest organization in the world devoted to ending the nuclear arms race.

Democratically organized, FAS is currently composed of 3,500 natural and social scientists and engineers interested in problems of science and society.

FAS's four and a half decades of work as a conscience of the scientific community has attracted the support of the distinguished Sponsors listed below.

SPONSORS (partial list)

*Sidney Altman (Biology)
*Philip W. Anderson (Physics)
*Christian B. Anfinsen (Biochemistry)
*Kenneth J. Arrow (Economics)
*Julius Axelrod (Biochemistry)
*David Baltimore (Biochemistry)
Paul Beeson (Medicine)
Lipman Bers (Mathematics)
*Hans A. Bethe (Physics)
*Konrad Bloch (Chemistry)
*Norman E. Borlaug (Wheat)
Anne Pitts Carter (Economics)
*Owen Chamberlain (Physics)
Abram Chayes (Law)
Morris Cohen (Engineering)
Mildred Cohn (Biochemistry)
*Leon N. Cooper (Physics)
Paul B. Cornely (Medicine)
Carl Djerassi (Organic Chem.)
*Renato Dulbecco (Microbiology)
John T. Edsall (Biology)
Paul R. Ehrlich (Biology)
George B. Field (Astrophysics)
*Val L. Fitch (Physics)
Jerome D. Frank (Psychology)
*D. Carleton Gajdusek (Medicine)
John Kenneth Galbraith (Economics)
Richard L. Garwin (Physics)
*Walter Gilbert (Biochemistry)
Edward L. Ginzton (Engineering)
*Donald Glaser (Physics-Biology)
*Sheldon L. Glashow (Physics)
Marvin L. Goldberger (Physics)
*Dudley R. Herschbach (Chem. Physics)
*Alfred D. Hershey (Biology)
William A. Higinbotham (Physics)
Roald Hoffmann (Chemistry)
John P. Holdren (Energy/Arms Con.)
*Jerome Karle (Physical Chemist)
*H. Gobind Khorana (Biochemistry)
*Arthur Kornberg (Biochemistry)
*Willis E. Lamb, Jr. (Physics)
*Leon Lederman (Physics)
*Wassily W. Leontief (Economics)
*William N. Lipscomb (Chemistry)
Roy W. Menninger (Psychiatry)
Robert K. Merton (Sociology)
Matthew S. Meselson (Biochemistry)
Neal E. Miller (Psychology)
Philip Morrison (Physics)
Richard A. Muller (Physics)
*Daniel Nathans (Biochemistry)
Franklin A. Neva (Medicine)
*Marshall Nirenberg (Biochemistry)
*Severo Ochoa (Biochemistry)
*Linus Pauling (Chemistry)
*Arno A. Penzias (Astronomy)
Gerard Piel (Sci Publisher)
Charles C. Price (Chemistry)
Mark Ptashne (Molecular Biology)
*Edward M. Purcell (Physics)
George Rathjens (Political Science)
*Burton Richter (Physics)
David Riesman, Jr. (Sociology)
Jeffrey Sachs (Economics)
Carl Sagan (Astronomy)
*Arthur Schawlow (Physics)
*J. Robert Schrieffer (Physics)
*Julian Schwinger (Physics)
*Glenn T. Seaborg (Chemistry)
Phillip A. Sharp (Biology)
Stanley K. Sheinbaum (Economics)
George A. Silver
*Herbert A. Simon (Psychology)
Alice Kimball Smith (History)
*Henry Taube (Chemistry)
*Howard M. Temin (Microbiology)
*James Tobin (Economics)
*Charles H. Townes (Physics)
Frank von Hippel (Physics)
*George Wald (Biology)
Myron E. Wegman (Medicine)
Robert A. Weinberg (Biology)
Victor F. Weisskopf (Physics)
Jerome B. Wiesner (Engineering)
Robert R. Wilson (Physics)
C.S. Wu (Physics)
Alfred Yankauer (Medicine)
Herbert F. York (Physics)

*Nobel Laureate

NATIONAL COUNCIL MEMBERS (elected)

Barry M. Casper (Physics)
Stephen F. Cohen (Pol. Science)
Denis Hayes (Engineering)
Gerald J. Holton (Physics)
Thomas L. Neff (Physics)
George W. Rathjens (Pol. Science)
Barbara Rosenberg (Biochemistry)
Arthur H. Rosenfeld (Physics)
Martin J. Sherwin (History)
Lawrence Scheinman (Law-Pol. Science)
J. David Singer (Pol. Science)
Valerie Thomas (Physics)

Ex Officio: John P. Holdren, Matthew S. Meselson

FAS FUND

The Federation of American Scientists Fund, founded in 1971, is the 501 (c)(3) tax-deductible research and education arm of FAS.

Frank von Hippel, Chairman
Moshe Alafi
Ann Druyan
William A. Higinbotham
Proctor W. Houghton
Jeremy J. Stone, President
Rosalyn R. Schwartz
Martin Stone
Alan M. Thorndike
Robert Weinberg
Raymond S. Sczudlo

The *FAS Public Interest Report* (USPS 188-100) is published bi-monthly at 307 Mass. Ave., NE, Washington, D.C. 20002. Annual subscription $25/year.

Copyright © 1993 by the Federation of American Scientists.

POSTMASTER: Send address changes to FAS, Public Interest Rep., 307 Massachusetts Avenue, NE, Washington, D.C. 20002.

THE CLINTON SECRECY REFORM INITIATIVE

On April 26 President Clinton issued a directive that establishes an official classification reform process. A task force, composed primarily of classification officials from the Reagan and Bush Administrations, has been assigned to address a series of questions and to prepare a new executive order on the classification of national security information. These questions, and our reflections on some possible answers, are presented below.

In the post-Cold War era, what types of information continue to require protection through classification in the interest of our national security?

This seemingly straightforward question has profoundly contentious depths, since its answer depends upon the meaning of national security, an ill-defined and widely abused term.

In a landmark 1956 decision, *Cole v. Young*, the U.S. Supreme Court said that national security pertains "only to those activities which are directly connected with the Nation's safety, as distinguished from the general welfare." Further, national security "was intended to comprehend only those activities of the Government that are directly concerned with the protection of the Nation from internal subversion or foreign aggression and not those which contribute to the strength of the Nation only through their impact on the general welfare."

By this definition, national security is essentially limited to protecting the nation or its allies from physical attack. It would appear to exclude virtually all other political activities, let alone budgetary, environmental or historical matters.

Classification in the interest of national security would therefore be applicable only to information directly related to military defense. That is one possible answer to our question, although the character of the post-Cold War military threat to the nation, and the role of information in protecting against that threat, remain to be determined.

Many other answers are possible. As the definition of national security expands, its implications become blurred. If national security includes economic vitality, should more information be classified to fortify U.S. industry, or should more information be declassified and freely accessible in order to spur innovation? If national security depends on an informed and politically aware electorate, could classification itself be a threat to national security? And who decides?

Fortunately, it is not necessary to provide final answers to these questions in order to correct most of the failures of the present classification system. That is because the majority of documents now classified need not be protected under *any* definition of national security.

In other words, disclosure of the majority of documents now classified—and nobody even knows how many there are—could not have any adverse effect on military defense of the nation today, or on current foreign relations, or even on the nation's "general welfare." Most of these documents have been classified reflexively or by rote, and more often than not, they are never declassified.

But how should classification proceed in the future?

The classification system does not exist in a vacuum. If it enhances national security, it also exacts a price from the nation. There are the literal costs of classification, secure storage and transmission, and declassification, which have become non-trivial as the secrecy system has expanded dramatically. And there is the more obscure, but potentially more damaging cost of insulating government activity from public awareness.

In view of these costs, nothing should be automatically classified merely by virtue of its "type" or category. Under some conceivable conditions, almost any type of information could have importance for public policy and debate. At the same time, however, some information could genuinely cause damage to the safety and security of the nation. The following sorts of information therefore should be *eligible* for classification:

- Details of advanced weapons system design and operation (though obviously *not* including their existence or program costs)
- Details of pending military operations
- Details of ongoing diplomatic negotiations
- Identity of confidential intelligence sources that could be jeopardized by disclosure, cryptographic methods in intelligence, and operational characteristics of advanced intelligence technologies

Any such information should be classified only when the risks of disclosure clearly outweigh any public interest in the information. This consideration was known under the Carter Administration as the "balancing test." It recognizes that there are times when the public interest requires disclosure even of information that could pose a threat to the nation. The balancing test provision was abolished by the Reagan Administration.

What steps can be taken to avoid excessive classification?

Excessive classification means that information is classified when it doesn't need to be, or that it is classified at a higher level than necessary, or that it remains classified when it no longer warrants protection.

One simple means of reducing excessive classification is to require that whenever classification is imposed, the basis for that action should be precisely specified, indicating the manner in which disclosure would damage national security. This will help compel reasoned classification decisions and allow meaningful application of the balancing test, engender new respect for classification restrictions, and facilitate timely declassification.

(continued on next page)

As noted by Arvin S. Quist, in a major new study of classification principles performed for the Department of Energy, "There should be a definite, identifiable reason or rationale for classifying information or materials. If a reason cannot be expressed or can only be given in vague terms, then the information or material probably should not be classified." (*Security Classification of Information*, vol. 2, "Principles for Classification of Information," April 1993, National Technical Information Service, page 15)

But as long there is confusion about what is properly classified, there will necessarily be disagreement about what constitutes excessive classification. In practice, there

Appoint an Anti-Secrecy Czar

Why, despite the new Clinton Administration review, and the end of the Cold War, are anachronistic patterns of government secrecy likely to resist effective reform unless the effort is led by a single, high-level individual: a czar of classification reform?

The failure to control government secrecy has, after all, persisted for decades. In 1956, a Defense Department committee was already complaining that "overclassification has reached serious proportions." In 1972, President Nixon concluded that the Cold War secrecy system had "failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time." By 1985, after three purported reforms of the classification system under Presidents Nixon, Carter and Reagan, a blue-ribbon commission still found that "too much information appears to be classified and much at higher levels than is warranted."

But why a czar? Consider the question of automatic declassification, a policy explicitly endorsed by Presidents Eisenhower, Kennedy, Nixon and Carter, but never successfully implemented. This sensible approach ties document declassification to the passage of a certain period of time, without requiring a laborious and costly review.

When President Carter mandated automatic declassification after six years of most secret documents, classification bureaucrats invented a new, unauthorized practice of a six-year "review," with the result that 90 percent of the affected documents were never automatically declassified.

A secrecy reform czar, in contrast, could examine exactly how past declassification efforts were evaded and could, with the cunning of a single mind, formulate methods of implementation that effectively anticipate future evasions.

Or take the problem of industrial security, in which contractors must comply with multiple, conflicting secrecy procedures of the various agencies with which they work. President Bush assigned an interagency task force of the National Industrial Security Program, composed of eleven working groups and hundreds of individuals, to develop a "single, integrated, cohesive" industrial security program. A secrecy reform czar would have had a fighting chance to reconcile the competing interests and achieve this worthy goal.

Instead, the participant agencies and contractors, jealous of their autonomy and their lucrative secrecy budgets, fell short of their goal. Though some progress towards simplification was made, they nevertheless decided that there were "special classes of classified information," and proceeded to define unique requirements for each of them, in defiance of their original task.

Or take the problem of "special access programs," in which customized security procedures add cost and complexity to an already baroque government secrecy system, effectively concealing many programs even from Congress. But Congress itself proved unable or unwilling to dismantle the system even though its legislative function was undermined by its inability to effectively monitor such hyper-secretive programs. This confirms that the system cannot reform itself without some innovation.

It is not beyond the ability of a single, highly-skilled systems analyst, with suitable staff and resources, to make the myriad political and technical judgments and tradeoffs involved. Secretary Robert McNamara made far more numerous and challenging decisions than these when he ran and revamped the Department of Defense.

At the end of the secrecy reform czar's review, both the White House and the Congress would have at their disposal a well-founded basis for proceeding to recast the regulations and statutes involved. In particular, the czar would be able to champion the decisions he or she made by explaining those judgments to the President and by testifying to the Congress.

Since blue ribbon and interagency panels, charged with implementing traditional presidential initiatives, have repeatedly failed, one must ask whether the battle has thus far been improperly joined. In organizational terms, such panels represent only small bureaucracies challenging much larger and more entrenched bureaucracies. And the presidents seeking reform, who do represent decisive authority, are invariably preoccupied with other, more time-urgent tasks.

Thus, for the same reasons that led the President to assign Hillary Rodham Clinton to devise a health care plan, a secrecy reform czar could be the appropriate organizational response. —*JJS*

■

will always be a subjective factor in applying classification standards.

The true solution to excessive classification is the creation of a culture of openness throughout government. Where there was reflexive secrecy and mindless classification, there should be a predisposition to open government. Creating such a predisposition is no easy task, and will not be accomplished merely by Executive Order, although the quality of the forthcoming Order will send an important signal, for good or for ill.

Purging our political culture of unnecessary secrecy is of course not a new challenge, and it may never be finally completed. But it is at least incrementally achievable. Important steps have been accomplished in the past, as with the introduction of the Freedom of Information Act in 1966.

As one senior classification official recalled, "There was a transition period that I grew up in from 1970 through the next decade where you had lots of people who had worked in the government since the 1940s, and who just weren't going to accept the fact of the Freedom of Information Act. You would hear them say, 'I'll decide what the public gets to know.' That has changed. In the early 1970s, a lot of people said it that way."

Any future transition away from excessive classification will take time. More important, it will take the kind of leadership and commitment to open government and democratic decision-making that have been lacking for years.

What steps can be taken to declassify information as quickly as possible?

If there is no fully satisfactory "blueprint" for classifying information properly, at least the damage done by excessive classification can be mitigated by prompt declassification. This should be accomplished by adopting the practice of automatic declassification, by which all or most documents are declassified after the passage of a predetermined period of time, without requiring individual declassification review.

Remarkably, some type of automatic declassification procedure has been advocated or accepted by most presidents since the early days of the Cold War classification system, though it has never been successfully implemented.

In 1953, President Eisenhower directed that "to the fullest extent practicable," a specific date or event should be cited at the time a document is classified, after which it would be automatically downgraded or declassified. (Executive Order 10501, sec. 4a)

In 1961, President Kennedy revised and elaborated this provision, based on the diversity of categories of national security information and the differing degrees of threat they may pose. Thus, information originated by foreign governments, information controlled by statutes such as the Atomic Energy Act, as well as intelligence and cryptography were all to be exempt from automatic procedures (though they were still ultimately subject to declassification).

There was also a vague exemption for unspecified "extremely sensitive information" that could be individually designated by agency heads. Another category of information could be deemed sensitive for an indefinite period yet would still be automatically downgraded to the lowest classification level, though not automatically declassified. Finally, everything else was to be automatically downgraded at three year intervals, and automatically declassified twelve years after issuance. (E.O. 10964, section 1)

In 1972, President Nixon declared that Kennedy's system had "failed" to bring about timely declassification. He defined an even more incisive general declassification schedule by which Top Secret information would be downgraded to Secret after two years, to Confidential after two more years, and declassified after a total of ten years. Similarly, information originally classified as Secret would be declassified after a total of eight years, and Confidential information after six years.

Nixon allowed for the possibility that some exceptional classified information "may warrant some degree of protection" beyond the scheduled declassification period. Such exceptions had to be approved in writing along with an ultimate declassification date, were to "be kept to the absolute minimum," and were limited to four specified categories: foreign government information; statutorily protected information; information on a system, plan, or project whose protection is essential to national security; or classified information that would place a person in immediate jeopardy. (E.O. 11652, section 5)

In 1978, President Carter directed that automatic declassification should occur not more than six years from the date of classification. Senior officials were granted authority, to be used "sparingly", to extend the period for declassification to no more than twenty years after classification, and no more than thirty years for foreign government information. (E.O. 12065, section 1-4)

In 1982, President Reagan all but abolished automatic downgrading and declassification. Furthermore, he permitted automatic declassification decisions effected under previous Executive Orders to be invalidated at the originating agency's discretion. (E.O. 12356, section 1.4)

Some general lessons emerge from this history. First, the diversity of types of classified information always dictated the possibility of exceptions and exemptions. It was never deemed possible to employ a fully automatic declassification system. On the other hand, until the Reagan era it was always recognized that some form of automatic declassification was desirable and, in fact, necessary for the system to function properly.

But automatic declassification has never been successfully implemented, as the national security bureaucracy has tended to ignore or to defeat even the most explicit directions from any president.

Thus, according to Steven Garfinkel of the Information Security Oversight Office, "The Carter idea of six year automatic declassification was a fiction— the system just didn't do it. Classifiers created this fiction called six year review which was not provided for in the Carter order.

What we ended up seeing was that more than half of the documents classified were marked for six year *review* rather than six year *declassification*. And then you add to those the ones that were marked for twenty year review, which was an exception" allowed by Carter.

"By the time you added all these 'exceptions' together," said Garfinkel, "you got over 90 percent of the material being marked as an exception. And so it was really a fiction. . . . The same thing happened with the Nixon order. Most of it was marked in the excepted category."

Thus, in the past, automatic downgrading and declassification did not work very well even when there was a President who favored it. This suggests the need for an enforcement mechanism beyond the issuance of a Presidential Directive, or the nominal enforcement provisions previously put in place.

Such enforcement might be assigned to a more aggressive, cabinet-level version of the existing Information Security Oversight Office. Alternatively, the Inspector General Act could be modified to direct each agency's Inspector General to monitor and enforce compliance with declassification procedures.

Some effort might be made to accommodate the concerns of different agencies by establishing different declassification schedules for different types of information. But the principle of automatic declassification must remain intact.

To ensure the effective functioning of an automatic declassification program, there should be a quota on exceptions. Since not all classified documents are created equal, some allowance for exceptions to the rule of automatic declassification will have to be made. But to prevent the exceptions from becoming the rule, they should not be permitted to exceed a certain quota or fixed fraction of the total. Further, they should require written justification from a responsible senior official, and be subject to independent review.

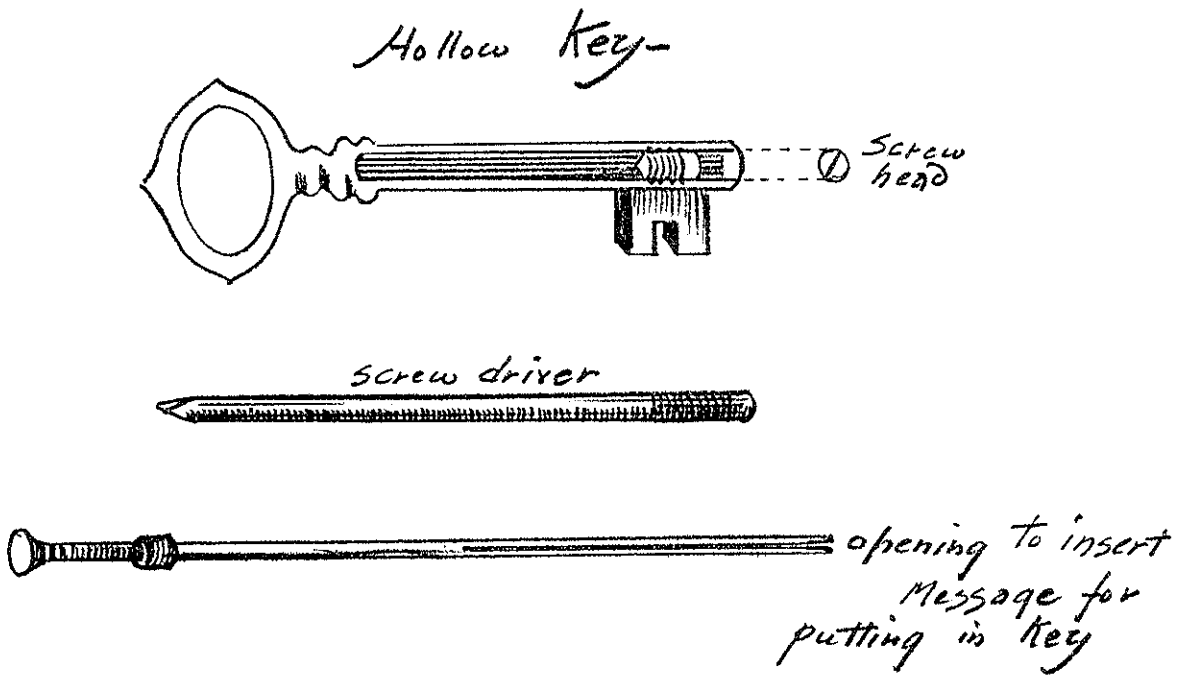
Some declassification review will still be required in exceptional cases, and when document declassification is requested in advance of the scheduled automatic declassification date. In order to eliminate the wasteful, time-consuming practice of independent multi-agency declassification review of many documents, a form of "universal on-site declassification authority" should be established so that declassification may be executed by a single review at a single agency.

In other words, the agency in possession of a document, even if it is not the originating agency, should be authorized in most cases to declassify it. This step alone would dramatically shorten the time needed to declassify many documents.

What steps can be taken to declassify or otherwise dispose of the large amounts of classified information that exist in Government archives and other repositories?

It is essential that older documents be declassified in bulk, that is, without painstaking individual review.

In 1991, FAS learned from the National Archives that the oldest classified military document in their possession dated back to April 15, 1917, shortly before the U.S. en-



This World War I "intelligence method"—a hollow key for transporting secret messages—remained classified for 75 years. The accompanying text from 1917 notes that "These keys are so constructed that by putting cigar ashes in the end after re-screwing with a communication inside, it is impossible to detect." Numerous other documents from the World War I era remain inaccessible to the public, ostensibly on national security grounds.

tered World War I. Remarkably, this document had been reviewed as recently as 1976 and exempted from declassification.

We requested a copy of the report, which concerned intelligence activities in Europe, under the Freedom of Information Act. After the passage of eight months, it was finally declassified in its entirety. Several other documents from the *very same day* in 1917, however, remain classified.

No one even attempts to defend the continued classification of such documents, but resources have not been sufficient to win their release through individual declassification review.

There is a consensus that after the passage of some period of time, no document merits continued classification in the interest of national security, and no declassification review is needed to confirm that fact. (Information that is specifically classified by statute, such as nuclear weapons design data, is an exception to this rule.)

The middle ground of this consensus holds that all classified documents older than twenty years should have their classification cancelled. In his 1978 classification directive, President Carter ordered that documents not automatically declassified under the standard six-year declassification schedule should be declassified, in most cases, no more than twenty years after original classification.

There was an exception for foreign government information, which could remain classified up to thirty years. Historians generally agree the cancellation period should be thirty years. The former head of the National Archives suggested forty years.

In a recent letter (*Issues in Science and Technology*, Fall 1992) Edward Teller proposed that all classified documents be released after one year. "Let us pass a law requiring all secret documents to be published one year after their issuance. This would of course eliminate long-term secrecy and might also deter unnecessary classification of documents, because the original invocation of secrecy might be subject to criticism and even ridicule when the documents are published."

"A short time ago, the Soviet Union was the most secretive organization in the world; it no longer exists," Teller wrote. "This puts the United States in the uncomfortable position of holding the record in secrecy. It is urgent that we do something about this situation."

What steps can be taken to reduce the number of, and provide adequate oversight and control over, special access programs?

The special access classification system involves secrecy measures even more stringent, and more subject to abuse, than the standard system with its classification levels of Confidential, Secret, and Top Secret. In many cases, unique physical protection requirements and access procedures are imposed to the point that independent oversight, due process standards, and even good management principles are seriously compromised.

(continued on page 8)

Inspector General Audit on Timberwind

In an extraordinary confirmation of what has become conventional wisdom, the Defense Department Inspector General (IG) found that the decision to establish the Timberwind nuclear rocket program as a special access program (SAP) in 1987 "was not adequately justified." Furthermore, the Strategic Defense Initiative Organization "continued to safeguard its association with the technology for reasons that were not related to national security."

Discovery of the highly classified Timberwind program helped inspire the current FAS project on government secrecy, since the classification of the program seemed so manifestly excessive. The 75-page Inspector General report, initiated in response to a complaint by FAS in September 1991 and published in January of this year, provides a rare and disquieting look into the SAP world.

"The decision to protect SDIO's development of a nuclear propulsion technology within a special access program was questionable. SDIO did not adequately justify why the existing control system . . . was not sufficient to protect the development of the technology. Although this was required by [DOD regulations], the Office of the Secretary of Defense did not enforce the requirement.

"The DOD initiated the program in secrecy, limiting open discussion and debate on the feasibility of using this technology for an SDIO mission by the mid-1990s, the safety factor involved in using a nuclear propelled missile interceptor, its cost, and other applications of the nuclear propulsion technology."

Some broader implications of the report are deeply disturbing:

- **The IG investigated Timberwind only after receiving the complaint from FAS, which was not even authorized to know of the program's existence. In the absence of the complaint, no investigation would have ensued.**
- **Top DOD officials all reject the IG's conclusions. Indeed, half the report is devoted to lengthy rebuttals from senior Pentagon officials. Although the IG stood by its findings for the most part, the rebuttals indicate that the Pentagon has a distorted and self-serving view of what justifies special access status. For that reason, it is likely that many other SAPs are similarly unjustified.**
- **Congress funded Timberwind for four years on a special access basis without protest. There is still no effective mechanism for Congress to determine the justification or propriety of special access status. A recent GAO report on special access programs looked at Timberwind but totally missed its improper classification, or the relation between excessive secrecy and the failure of the program.** ■

The special access system must be drastically curtailed, and ultimately eliminated. As a first step, all weapons acquisition programs—which have proven to be the most troublesome category— should be removed from special access status.

Agency heads are authorized by the current Executive Order to create special access programs (SAPs) when they believe that ordinary classification will not provide enough secrecy. In the 1980s, as confidence in the regular classification system declined, more and more programs were put in the special access category, which allowed for unique restrictions on access, above and beyond those of regular classified programs.

The very uniqueness of the SAP security requirements aggravated the complexity of the classification system, drastically increasing costs. The SAP classification system has also frustrated Congressional oversight, and contributed to fraud and abuse, most famously perhaps in the collapse of the A-12 aircraft program, which cost taxpayers over a billion dollars.

As the House Armed Services Committee put it in 1991, "The special access classification system . . . is now adversely affecting the national security it is intended to support." As part of the effort to restore some degree of propriety to the classification system and to cut unnecessary security costs, the Clinton Administration should move to eliminate the special access classification system.

Special access procedures significantly undercut legislative oversight efforts. There is only a relative handful of Congressional staff members who are cleared for access to most "black" programs. Even if the staffers are exceptionally competent, it is an impossible task for them to effectively conduct oversight on hundreds of special access programs, particularly since the very programs that are seeking funding are the only available source of information.

All but eight members of the House and Senate are denied information about one category of special access programs, known as "waived" programs. In this situation, the Secretary of Defense "waives" his obligation to notify Congress about certain activities, except for the chairmen and ranking minority members of the House and Senate Armed Services Committees and Defense Appropriations Subcommittees.

Besides virtually nullifying the Constitutional separation of powers, this occasionally causes some grotesque confusion, as in the case of Aurora, the supposed hypersonic reconnaissance aircraft that some say is already in operational service [*see* September/October 1992 PIR]. One Congressman, Rep. Robert Walker (R-PA), recently suggested he might oppose funding for the National Aerospace Plane program because Aurora may now be flying. "If in fact that is the case, and it's been heavily rumored," Walker said, "we're spending a lot of money duplicating technology that may already be operational."

The Air Force vigorously denies that anything like Aurora is already in service or even in an advanced state of development. That is probably true. But the revealing point is that the official denial is not taken seriously, even by conservative members of Congress, just because there has been so much deception and disinformation about special access programs.

As noted above, the problems of inadequate oversight and, occasionally, contractor fraud, have mostly affected weapons acquisition programs that utilize special access procedures. The first priority for reform, therefore, should be to remove such programs from the special access system.

On the positive side, opening up the special access world at least a bit could help to promote the economic vitality which is increasingly important to the new conception of national security.

Having spent tens of billions of dollars on classified research and development in the last several years alone, there is a high probability that the Defense Department has achieved something worthwhile, including some research that would benefit the civilian technology base. Some of this work is apparently starting to emerge. But much of it is in danger of being lost or unnecessarily duplicated due to excessive secrecy.

According to Rep. Patricia Schroeder, chair of the House Armed Services research and technology subcommittee, there has been "tremendous overclassification" of defense technology since World War II. "A lot of people don't know what's been going on, mainly because it's secret."

Consequently, she said, rapid declassification is needed to help the U.S. compete in the commercial global marketplace. "We're trying to push very hard to make sure" this happens.

It would be easy to overestimate the value of military R&D for commercial applications. Most of it is likely to be targeted to specific military requirements that have no civilian analog. Much of it is likely to remain sensitive and subject to continuing security safeguards. But some of it—particularly in areas such as communications, data processing, propulsion, and materials science and engineering—may well have commercial and other value, if habitual secrecy practices can be overcome.

One remarkable sign of the times is the disclosure last April of Lockheed's "Bus 1," a hitherto classified military spacecraft bus, which is being contemplated for use by NASA on a reconfigured Space Station. [A "bus" is a support structure that provides power, propulsion and other services to the spacecraft payload.]

Although Bus 1, which is currently in production, has already been qualified for flight on the Shuttle, NASA says it doesn't know what program the system came from. According to FAS Space Policy Project Director John Pike, it was developed for a classified photoreconnaissance satellite known as the Advanced Keyhole.

NASA's disclosure of Bus 1 was accompanied by a surprising degree of technical detail, including design parameters that allow one to deduce its propellant loading and, hence, the duration of its multi-year lifetime. For an intelligence satellite system, this would ordinarily be considered properly classified information.

In a somewhat more unlikely application, a classified aerial reconnaissance system was used by biologists to monitor the population of sandhill cranes roosting along the Platte River in Nebraska.

The AN/AAD-5 infrared reconnaissance sensor was used in a cooperative effort between the Nebraska Air National Guard and biologists from the University of Nebraska and the U.S. Fish and Wildlife Service. The Guard, which routinely trained with the sensor anyway, agreed to monitor the Platte River as a training exercise.

"Individual cranes roosting in the river at night were readily visible" with the then-classified sensor, which "had better resolution and other characteristics" than unclassified sensors could provide, according to a new report on the project in the journal *Remote Sensing and Environment* (vol. 43, 1992).

"We were very fortunate to have had the collaboration of the Nebraska Air National Guard," Fish and Wildlife biologist John G. Sidle told FAS. "The Guard acquired their necessary training while we got a valuable product for our Platte River conservation and regulatory efforts. I would hope that [other] DOD technology could be used" in similar efforts.

It remains to be seen if these developments are the precursors to a new wave of revelations of classified technology, or exceptions that prove the stubborn rule. In the meantime, there is reason to suspect that some black program developments will be lost altogether, as the result of excessive compartmentalization.

Many technology programs are so highly classified that their products are never archived in any kind of central repository, such as the Defense Technical Information Center, where other researchers could discover and benefit from them. Except for the huge sums of money spent to pay for them, they might as well never have existed.

What steps can be taken to control unnecessary distribution and reproduction of classified information? What steps can be taken to enforce the "need-to-know" principle?

Theoretically, to gain access to classified information, one must not only have a security clearance, but also a "need to know" the specific information in question. As a consequence of the diminished credibility of the classification system, the need to know principle has been commonly disregarded. (But it might be noted, in passing, that many of the most damaging espionage cases in recent years involved individuals who were both properly cleared and had a need to know.)

This is primarily an internal educational and management issue. But if fewer documents are improperly or unnecessarily classified, respect for the system will grow, and compliance with the need-to-know principle will increase.

It is interesting to observe that many government officials who willingly "leak" classified documents draw the line at releasing proprietary information. Recognizing the validity of proprietary restrictions, these officials are careful to obey restrictions on its disclosure. In contrast, the near-universal recognition that most classified documents could not possibly damage national security, in any plausi-

Bus 1 Overview

Design Characteristics

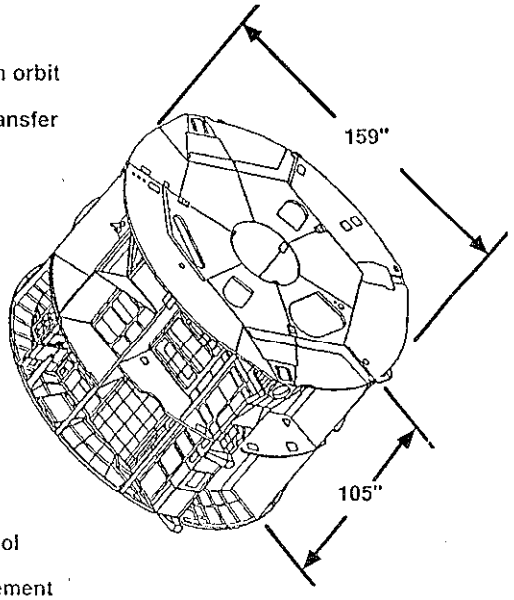
- Multi-year operation in low earth orbit
- Three -axis control plus orbit transfer

Status

- Qualified for STS and ELV
- Currently in production

Subsystems

- Structures and Mechanisms
- Propulsion
- Electrical Power
- Guidance, Navigation and Control
- Communications &Data Management



The highly classified spacecraft module known as "Bus 1" was abruptly declassified last April and proposed for use in a reconfigured Space Station. It is likely that the classified industrial base holds a number of technologies that could be productively utilized for civilian applications.

ble meaning of the words, has produced contempt for the system and a cavalier attitude towards compliance.

Broad distribution of classified information also complicates the declassification process, often leading to multiple declassification reviews of the same document. Establishment of centralized indices of declassified documents should be considered to address this problem. A reduction in the scope of classification activity will also help to simplify the situation.

What steps can be taken to increase individual accountability for the operation of the classification system?

One simple answer is that those who do the original classifying should be identified on the documents, along with a citation of the precise basis for classification (as well as an automatic or other declassification date). Individuals who habitually overclassify, even in good faith, should lose classification authority.

According to Robert D. Steele, formerly a senior Marine Corps intelligence officer, "It has been my experience that employees of the various intelligence community organizations routinely classify everything they collect, everything they write. This is in part because there are severe penalties for underclassifying information, and there are no penalties of overclassification, even if overclassification is against the public interest."

Clearly, the classification system needs to be restructured in such a way that incentives are in place for eliminating unnecessary classification, and substantial disincentives—including penalties—are in place for overclassification.

But a far more important question is how to improve oversight and accountability of the classification system itself. Plainly, the existing oversight procedures are not working.

The current classification system, based on President Reagan's Executive Order 12356, already dictates that "Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security."

Furthermore, "In no case shall information be classified to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security."

Since the Reagan Order was issued in 1982, hundreds of documents from the World War I era, to cite just one example, have remained classified. Either they still "require protection in the interest of national security"—which is absurd—or the Order is being continuously violated.

The Order authorizes sanctions for violations of its requirements. But there is no evidence that they are ever employed. We asked Steven Garfinkel, Director of the Information Oversight Office, if anyone had ever been terminated for overclassification? The answer was, "No." Has anyone ever lost classification authority for overclassifying a document? "Not that I'm aware of." But neither have huge volumes of egregiously overclassified documents been downgraded or declassified.

This is an urgent and fundamental problem. If uncorrected, it will mean that even a brilliantly crafted new Executive Order that appears to eliminate unnecessary secrecy may never be effectively implemented and enforced.

The need for some structural improvements in oversight is clear. The current Information Security Oversight Office is inadequate. Even assuming it has the will and the proper intention, it does not have the resources to oversee the huge secrecy bureaucracy.

More important, it does not have the clout. As an obscure entity buried in the General Services Administration, it is in no position to effectively challenge the entrenched powers of the defense or intelligence agencies, for example, no matter what its charter might say.

As Robert Steele observed in recent testimony, "I have never, in eighteen years of experience [in the intelligence community], encountered a representative of the Information Security Oversight Office, or heard of a spot check of any documents associated with any office I have ever been associated with. Although [the current Executive Order] provides ISOO with the authority to conduct on-site inspections, this does not appear to be a common practice. In my experience, the Information Security Oversight Office has been a 'zero,' irrelevant and ineffective."

The existing functions of the Information Security Oversight Office should be transferred to a Cabinet-level agency, perhaps the National Security Council. In addition, accountability needs to extend deep into the labyrinth of the classification system itself. Each agency head should appoint a dedicated authority, with suitable staff, to independently monitor compliance with classification standards, automatic declassification schedules, and other requirements.

The primary task of these oversight bodies should be to assure that classification activity is reduced to the minimum level necessary. Each agency's oversight authority should function independently of the agency's classification structure, as a built-in sort of self-check, and should be authorized to enforce compliance with the new Executive Order. Finally, an external oversight body, including public representation, should be established to conduct top-level oversight and to resolve disputes about the appropriate limits of classification.

Ultimately, however, the proper functioning of the classification system cannot be fully prescribed in any Executive Order, no matter how detailed, or even legislated into law. It will require a new orientation of our political culture, based on the notion that citizens have a fundamental right to know about the conduct of their government's activity, a right that may be infringed upon only on an exceptional basis, and only on grounds that are consensually recognized to be justified. —*Steven Aftergood* □

LOOK WHO'S CRITICIZING EXCESSIVE SECRECY

Until recently, most criticism of the national security classification system was expressed by journalists, civil libertarians, scientists, and frustrated FOIA requesters. Increasingly, however, the national security establishment itself, and those who are obliged to implement the secrecy system, are acknowledging that excessive secrecy is harming the nation and insisting that it be reversed.

Military Space Officials

In 1992, Vice President Dan Quayle commissioned a task group of the Space Policy Advisory Board to review the nation's space policies in the context of the end of the Cold War. The group included several former leaders of the national security space program, a former Secretary of the Air Force, the current chairman of the Defense Science Board, and other military and civilian space policy experts. Their December 1992 report, entitled "A Post Cold War Assessment of U.S. Space Policy" and excerpted below, focused repeatedly on the adverse effects of excessive secrecy.

"The security classification requirements created to protect U.S. space and intelligence capabilities during the Cold War contribute to inefficiencies in the conduct of the nation's space program and limit the broader utility of certain systems. With the end of the Cold War, the original rationale for many of the current security safeguards is less compelling and the potential benefits from removing many security constraints are substantial."

"Security constraints drive up the cost of U.S. government space programs in many ways. Physical and personnel requirements and their administration necessitate special building construction, extensive background checks, and systems for producing, processing, and storing material. They restrict the transfer of technical knowledge within the government and to and within industry."

"U.S. industrial competitiveness in the world marketplace is also affected because, for the most part, foreign sales and commercial spin-offs of highly classified space capabilities are not allowed."

"Relaxing security constraints could: enable industry to more easily move employees between civil and national security development programs; ensure that technology and experience developed for one government application are easily transferable to other government or private sector applications; reduce the overhead costs associated with maintaining strict physical and personnel security; and increase the data available to support public benefit applications."

"Current government guidelines regarding the classification of national security space activities, including secrecy surrounding organizational and contractual relationships, the existence and capabilities of space programs, operating procedures, and technology, increase costs, restrict coordination and cooperation, and limit opportunities for productive synergism."

Therefore, the President should "seek to reduce, and where possible eliminate, security constraints associated with national security space programs."

The National Archives

The National Archives maintains a backlog of many hundreds of millions of pages of documents thirty years old or older that await declassification review. The vast majority of these documents certainly merit immediate declassification, but the financial costs of maintaining and actually conducting declassification review of the backlog are practically insupportable. Following are excerpts from a 22 March 1993 letter sent by Acting Archivist of the United States Trudy Huskamp Peterson to National Security Adviser Anthony Lake.

"As you review the many issues facing the National Security Council today, I urge you to consider a fundamental revision of the Executive Branch's procedures for declassification of information. The system that has evolved since the Second World War weighs the risk of disclosure of information more heavily than the benefit of release to the American people. It is time to redress this balance."

"The public and the Congress are becoming increasingly impatient with the slow progress of release of documents. To name just one example, using personnel from both the State Department and the National Archives, we estimate that it will take nineteen years to review for declassification the State Department records created during the period 1960-1963. This is intolerable."

"While many suggestions have been made, and I am sure will be discussed in the months ahead, one revision is critical: a date certain when documents can be released. We at the National Archives hold hundreds of documents that pre-date the Second World War and remain classified by instruction to us of the originating agencies. Just last year we declassified our oldest classified document—an item from 1917—but other documents from the World War I era remain classified."

"Not only does this deny the American public the information contained in these items, but it requires needless administrative expense to house the classified items in secure storage, to handle the paperwork when they are requested under the Freedom of Information Act, and to make copies and return them to the agencies of origin when requested for review. In the effort

(continued on page 12)

(continued from page 11)
to make government more efficient, this obvious inefficiency should be eliminated."

Classification Officials

The National Classification Management Society is a thirty-year-old organization of classification officials and other information security specialists. Its goals include fostering "informed use and application of the security classification management and safeguarding processes of government and industry." Following are excerpts from a 30 September 1992 letter sent by NCMS in response to a request from the Central Intelligence Agency Task Force on Classification Standards.

"When we invoke national security as the basis for classification, we are asking for public trust that what is being done is in the best interest of the nation and its people. That trust has been violated too many times from all appearances.

"The special controls on intelligence information not only make it difficult to use, but they make working with it for those with access authorization more time-consuming and expensive. . . . With the redefinition of the threat, many of these rules need to be reconsidered with a view toward simplification."

"[The classification label] 'Originator Controlled' (ORCON) is a special problem. We have experienced many instances in which intelligence estimates or products had to have essential information left out because some of the most vital reports were labeled ORCON. The final products were misleading because the information that would give the true situation was ORCON and not available for broader use in a timely fashion. Often, we are unable to see any reason why reports should have the ORCON label except for caprice."

"We are not necessarily uncomfortable with the amount of material classified. It is better that something innocuous be classified than that something vital be released. But playing it safe in this way leads to excessive classification. The penalty for a mistake has always been [for releasing] something when it should have been protected. That needs to be counterbalanced by some penalty [when] clearly unclassified information is labeled as classified."

"The amount of compartmentalization and number of compartments probably are excessive. Compartmentalizing leads to some very unintelligent intelligence activities."

"The cost of handling and using intelligence information should be lowered by more realistic procedures for protection of the information."

"The cost of classification should not be considered separately from the cost of security. The cost of classification *per se* is relatively small but the cost of security is driven by classification and both should be considered together. Because the classification decision is the driver, those who are authorized to make classification decisions need to be instructed in the process and educated about the consequences of it, including the economic impact on the nation's ability to compete in the world marketplace. Classification by rote must be eliminated from the intelligence community and elsewhere." ■

FAS PUBLIC INTEREST REPORT (202) 546-3300
307 Mass. Ave., N.E., Washington, D.C. 20002
Return Postage Guaranteed
July/August 1993, Volume 46, No. 4

Second Class Postage Paid at Washington, D.C.

☐ I wish to renew membership for the calendar year 1993.
☐ I wish to join FAS and receive the newsletter as a full member.
Enclosed is my check for 1993 calendar year dues.

☐ $25 Member ☐ $75 Supporting ☐ $150 Patron ☐ $1000 Life ☐ $12.50 Student/Retired

Subscription only: I do not wish to become a member but would like a subscription to:
☐ FAS Public Interest Report—$25 for calendar year.

☐ Enclosed is my tax deductible contribution of _____ to the FAS Fund.

NAME AND TITLE _____
Please Print

ADDRESS _____

CITY AND STATE _____
Zip

PRIMARY PROFESSIONAL DISCIPLINE _____