Federation of American Scientists
307 Massachusetts Avenue, NE
Washington, D.C. 20002

for more information:
Steven Aftergood
(202)675-1012

SECRECY & GOVERNMENT BULLETIN

To Challenge Excessive Government Secrecy and
To Promote Public Oversight and Free Exchange
In Science, Technology, Defense, and Intelligence

Issue No. 23
June 1993
ISSN 1061-0340

Clinton Orders Review of Classification System

In an April 26 Presidential Review Directive, the Clinton Administration initiated an official review of the national security information classification system (*New York Times*, 5/5/93, p.A18). It is the first step in the development of a new Executive Order to replace E.O. 12356, the foundation of today's classification system.

The Directive assigns chairmanship of the review to Steven Garfinkel of the Information Security Oversight Office (ISOO), who was responsible for classification oversight in the Reagan and Bush years. A public hearing has been set for June 9 and 10 in Washington to receive proposals for changes to the classification system (*Federal Register*, 5/20/93, p. 29480). Written comments should be sent to ISOO, Attn: PRD Task Force, 750 17th St, NW, Suite 530, Washington, DC 20006.

The Directive sets out a series of questions to be addressed in preparing a new draft executive order. These questions are reprinted below, along with a general notion of what we think the answers ought to look like.

In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security? What steps can be taken to avoid excessive classification?

Nothing should be automatically classified merely by virtue of its "type." Just about any type of information could have importance for public policy and debate under some conceivable circumstances. At the same time, some information could genuinely cause damage to national security. The following sorts of information should therefore be eligible for classification:

- Details of advanced weapons system design, operation, and vulnerability.
- Details of pending military operations.
- Details of ongoing diplomatic negotiations.
- Identity of intelligence sources that could be jeopardized by disclosure; cryptographic methods in intelligence; and operational characteristics of advanced intelligence technologies.

Even such information should be classified only when the hazards due to disclosure clearly outweigh any public interest in the information.

In any case, the basis for classification should be precisely specified, explicitly indicating the manner in which disclosure would damage national security. This will help compel reasoned classification decisions, engender new respect for classification restrictions, and facilitate timely declassification.

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

Return to the practice of automatic declassification, as promulgated by previous executive orders, by which most documents would be automatically declassified after the passage of some sensible period of time. A suitable incentive or enforcement mechanism will be required to assure compliance. (see S&GB 17).

To eliminate the wasteful, time-consuming practice of independent multi-agency declassification review of many documents, establish a form of "universal on-site declassification authority" so that declassification may be executed by the agency in possession of the document.

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

It is essential that older documents be declassified in bulk, since individual review of the vast multitudes of such documents is not practical. The classification of all documents older than twenty years should be cancelled.

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

As a first step, all weapons acquisition programs, which have proven to be the most problematic category, should be removed from special access status.

Special access programs are the most highly classified programs, and the most subject to abuse. In many cases, their very existence is a secret, undermining Congressional and other oversight. They include weapons acquisition programs, intelligence programs, and military operations. (see S&GB 19).

If it is possible to achieve a regular classification system that is effective, the special access system can be eliminated altogether with no loss of security.

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?

This is primarily an internal management issue. But if fewer documents are improperly or unnecessarily classified, respect for the system will grow, and compliance with prudent distribution principles will increase.

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

Classifiers should be identified on classified documents, along with a citation of the basis for classification (as well as a declassification date). Individuals who habitually overclassify, even in good faith, should lose classification authority.

In Summary

- The volume of classification activity (6.3 million classification actions in FY 92) must be sharply diminished by limiting classification to those records that could demonstrably damage national security, and only when such damage outweighs any public interest in the records.
- The classification of the untold millions or billions

of documents more than 20 years old should be cancelled by fiat, without a pointless declassification review.

- The majority of new classified documents should be strictly subject to an automatic declassification schedule, to prevent the further buildup of classified records and to facilitate their ultimate release without expensive, painstaking declassification review.
- The excesses of the special access classification system should finally be curtailed, firstly by removing all acquisition programs from special access restrictions.

Industrial Security Interview

Sometimes secrecy is actually used to protect national security. Some of the most clearly appropriate applications of secrecy involve the protection of advanced military systems and technology, though even here the net has been cast too broadly and declassification has lagged badly. To try to get a sense of where things are in this field, S&GB Editor Steven Aftergood spoke with Gregory A. Gwash, Deputy Director of the Defense Investigative Service (DIS) for Industrial Security. Mr. Gwash co-chairs a working group of the National Industrial Security Program (NISP). He holds graduate degrees in Far Eastern history and in law, and he formerly served with U.S. Army Special Forces. The interview, excerpted below, took place on May 12 at DIS headquarters in Alexandria, VA.

First of all, what is industrial security?

Gwash: Industrial security is the system of protecting classified information that is released to industry to perform classified contracts for the government. It's a system that includes information security, physical security, personnel security, and computer security principally.

Most people, I think, now agree that the government tends to classify information indiscriminately and has failed to declassify a lot of information in a timely fashion. Is the same thing true with respect to technology?

Gwash: Because of the "originating agency's determination required" (OADR) standard in the present Executive Order [which permits declassification only by the originating classifier], there is a time lag in the declassification of otherwise mundane technological information, simply because one can't find the originating authority or one just doesn't bother. So there's a lot of information that's obsolete in terms of classification. It may still be in the system in terms of the materiel, but it really no longer merits that kind of national security protection.

Doesn't that suggest that one step for reform ought to be to eliminate the OADR standard, that there needs to be a more universal declassification authority?

Gwash: I agree with that.

In my opinion, there should [also] be some time schedule for automatic downgrading and declassification-- I like the time schedule of six years from a couple of Executive Orders ago. There can be exceptions to that, and when they're merited the exception can be granted. But it should become an automatic thing. That way, people will classify information knowing that it in six years it will be downgraded and ultimately declassified and we will move information through the system; because it shouldn't be necessary to protect information that is twenty-five or thirty years old that relates to military hardware and technology.

National Industrial Security Program (NISP)

In the last DIS Annual Report, you wrote that "the NISP process will revolutionize many aspects of traditional industrial security, including providing for common security standards and reciprocal inspections by DIS, Energy, CIA and the SAPs." But several people I've talked to say the NISP is falling short of its goals, and in fact is shaping up to be a major disappointment. Some people say NISP has been sabotaged, mainly by the CIA and the SAPs, who are opposed in principle to streamlining and want to retain autonomous security authority. Can you say anything about that?

Gwash: I wouldn't want to agree or disagree with your statement that some people think it's been sabotaged. I think it's still a developing process. To the extent it was conceived during the Cold War and we're now facing different threats, we're all having a time dealing with that. But I wouldn't say it's been sabotaged or that it's doomed to failure. If the NISP comes to pass, it will certainly do all the things that I predicted.

I say if the NISP comes to pass, that's not to say that the Executive Order [12829] isn't real and we're not in the process of complying with it, but I'm concerned about the direction we're going, when there are several other competing interests moving in the same direction with the DCI-DOD Security Commission which has been informally announced...

Let me ask you about that. There seems to be a remarkable proliferation of new security commissions and working groups. Besides the NISP and the DCI-DOD Security Commission, there's the Acquisition Systems Protection Program, there's the Garfinkel task force on classification reform, and reportedly a new Vice Presidential Panel on Industrial Security. At some point, doesn't each additional "review" compound the problem, rather than promoting a solution?

Gwash: It certainly compounds the problem for us working stiffs in industrial security. We have worked hard for two years to develop principles for the NISP which now seem to be at risk because of all these high-level commissions that are going to propose new standards, new principles, new guidance.

A lot of the questions that the new panels are going to ask have already been asked in earlier panels, and what's worse, it's essentially the same people who have been assigned to ask the questions! It's hard to believe the answers are going to be new.

Gwash: Well, we face a different national security threat today than we did four to five years ago, with the demise of the Soviet threat. We certainly don't have a smaller task before us in national security. But it's clear that there's a need, a desire in the new Administration to take a fresh look at defense acquisition, the process of procurement, and whether or not security plays a helpful or a hindering role.

I don't doubt that the questions are legitimate, but from the outside it sure looks like the government is going about answering them in a roundabout manner.

Gwash: I'm concerned too. As I said, the work that's been done in NISP seems to be at risk now. If Mr. Garfinkel's commission's objectives are to question the foundations of classification, the threat environment in which we classify, and the basis for special access programs, then a lot of the work we've done may have to be redone.

The French Are Coming
The French Are Coming

What about the whole French espionage furor, which followed the recent disclosure of a French memo that appears to target U.S. defense contractors?

Gwash: It's very difficult for me to talk about it on an unclassified basis. I know what's in the newspapers and I think there's obviously more to what's going on than meets the eye.

Some of this concern has been generated by industry itself and its concern for defending its markets. The American defense industry is competing with the defense industries of our allies. Some of it is just industrial espionage that may include classified information.

Some of it is just natural competitive intelligence. Everyone wants to know what their competitors are up to.

Gwash: The problem with that is that while that sounds somewhat benign, when it gets into the areas of influencing or affecting the American defense contractor community and our industrial base, then it becomes a national security issue which has to be addressed. The

loss of the Soviet Union as the main enemy and the principal threat has required us to reevaluate just what is the threat.

If the threat is only the French, then it's not nearly so significant. I would also say, if it's true, who's surprised? The French have been spying on us since the French and Indian War.

Let me run a few things by you about the French memorandum itself. Let's leave aside the curious fact that a 1989 memo suddenly surfaces in April 1993 when the intelligence budget is under increasing criticism and pressure. It seems to me that the document itself is not very impressive as an espionage roadmap. Anyone who scans the trade press for a few weeks could do as well or better in terms of completeness. There's also no indication that the authors of the memo were aware of any of the unacknowledged SAPs that were underway at several of the contractors named. In other words, there's no indication of any covert penetration of those programs. It was also classified as Confidentiel Défense, which is a low-level French classification. All of which suggests to me that this document taken by itself is not very persuasive evidence of a major espionage threat.

Gwash: Well, I don't have any information about the authenticity of the document. But I agree with you that it doesn't convey information about the companies that isn't in the public domain. Whether or not it's intended to be a roadmap or a stalking horse for someone, I couldn't say.

What about the whole phenomenon of "friendly spies?"

Gwash: There's no question that we have been damaged by espionage or intelligence collection by countries that have been considered allies. Is this the kind of thing that should be considered the focus of our security countermeasures and counterintelligence? I'm not sure. I hope we don't lose sight of the big challenges, the big threats out there. There are still people with nuclear weapons pointed at us. So while it's important to protect our technological advantage from all collectors, there is still a need to assure ourselves that we know what the people with the nukes are doing.

Loss of Critical Technologies

Susan Tolchin wrote a rather startling article in *Issues in Science and Technology* (Spring 1993) where she stated that "DOD collects virtually no systematic data on defense dependencies [on foreign suppliers], on sales of subcontractors to overseas buyers, or on foreign sourcing or foreign items used in weapons systems." As a result, she argues, and the GAO has argued, critical U.S. technolgies are slipping away. Is it possible that our industrial security program is totally missing the boat?

Gwash: I would emphatically say no, DIS is not missing the boat. We have a program to detect and control foreign ownership, control, and influence, commonly known as FOCI. Any cleared company-- and we are only involved with companies that have security clearances-- any cleared company that comes under foreign ownership, control, or influence, is addressed, and protective measures are put in place. Whatever is necessary to protect that company or its technology is accomplished, or the facility clearance is withdrawn and the company is no longer eligible for access to classified information.

Now to the extent that a company without a security clearance, but which has technology of value to the United States, could be acquired by foreign owners, that is more in the domain of the Exon-Florio Amendment, and the CFIUS process.

I think that's what Tolchin was criticizing.

Gwash: But as far as a cleared facility is concerned, we require them to report any foreign acquisition, even 5% of their stock being acquired. In any case of foreign ownership of a cleared facility, DOD requires that the foreign owners exclude themselves from management of the company by a trust or a proxy. And every cleared company with foreign ownership, control, or influence that includes foreign representation in the facility has to have a technology control plan to protect that technology, all technology, from acquisition by the foreign investor or the foreign interest. We think it's fairly effective. There's always more that could be done, if resources were available.

The Threat

We talked about the fact that up to a few years ago, the major threat was the Soviet threat. Is there increasing clarity today about what the threat of the '90s is, or is it still an open question?

Gwash: I think we're probably prepared to address the threat now more than we were in the previous Administration, just because time has passed. In other words, the demise of the Soviet Union and the Warsaw Pact only occurred late in the Bush Administration. For the last few years, we have been casting about to determine what is the threat. How do we define it, is it bigger, smaller, more diverse? We're at the point now, where our leadership is looking for a new national security strategy, and that strategy will in part determine what they see as the threat.

I think obviously the kinds of threats posed by the problems in the Balkans, those are national security threats, but are they threats to our information? No. But how we are going to develop a military infrastructure and a defense strategy to deal with those kinds of threats may drive what information and technology has to be protected.

I think we need to give the new leadership some time. We don't even have all the seats filled in the Pentagon yet. I have a lot of sympathy for the leadership facing all these international and national issues hitting them all at once. I admire them for even giving Steve Garfinkel the classification reform mission. They could have easily delayed it for years while dealing with more pressing issues. Which is not to say that there isn't a need to address the classification problem. Clearly, Executive Order 12356 has outlived its usefulness.

I couldn't begin to speculate on what will be classified under the new Executive Order. I would hope that military weapon systems, their vulnerabilities and capabilities would continue to receive protection. We have been successful in pressing our military cases overseas in the last few years because of the technological edge that we have, and our edge is in large part in classified systems, some highly classified, some not so highly classified. I'd like to see that advantage for our troops in the field retained.

Classifying Basic Research

Gwash: While classification is not my area of responsibility, one of the failings of Executive Order 12356, in my personal opinion, is the general prohibition on classifying basic scientific research [not clearly related to national security]. That may sound a little draconian...

Reactionary.

Gwash: Yeah, reactionary, thank you. But I really think that we waste a lot of time trying to safeguard information after the horse is out of the barn, so to speak. Basic scientific research is discovered, developed, publicized, broadcast to the world, and then we try to apply classification to its military application. It's a nightmare. It creates the problem of classifying everything that pertains to the application. That's where you get into the problem of needing unacknowledged programs and the like.

Of course, if you start assuming every initial stage of research is classified until it is known to have no military relevance, the whole scientific enterprise is just going to collapse.

Gwash: Well, I appreciate that. Certainly, if we made every scientist sign a security agreement before he fired up his Bunsen burner, it would make scientific progress

difficult. But on the other hand, a lot of scientific research is funded by defense R&D money. And yet it's considered independent research and development and the contractor gets to do what he wants with it.

Patent Secrecy

Gwash: In some cases of a new invention, the only way the government can get a handle on it is to slap a patent secrecy order on it, which I have big personal problems with. I'm an inactive attorney and constitutional law is an area that I think as security specialists we often don't pay as much attention to as we should. Actions like this just feel to me like a violation of the Fifth Amendment and maybe the First Amendment. And yet these things have never really been adjudicated by the courts. The government has just been permitted to slap these things on, and courts will just stand back and say, you know, national security, we can't get involved. I think we've made a mistake.

For example, years ago I was involved-- as an inspector-- with a company in Chicago that had a patent secrecy order placed on it, and it basically put the company out of business. They had a security clearance, and they did something-- which I'm not at liberty to talk about even now-- and a secrecy order was put on it. The secrecy order was never turned into a contract or a procurement action, and so this idea just died. Somehow that doesn't seem right.

The Disloyalty Constant

The theoretical underpinnings of classification are elaborated in daunting detail in a new DOE contractor report, "Security Classification of Information, volume 2: Principles for Classification of Information," by Arvin S. Quist.

The report brings a new degree of conceptual rigor to the subject of classification. The author distinguishes, for example, between subjective secrets ("What number am I thinking of?") and objective secrets ("What is the trillionth digit of pi?"), and defines five steps for determining whether information should be classified. There is an altogether excellent chapter outlining the risks and benefits of classification, a subject also treated in volume 1 of this report, dated 1989.

Occasionally, the author's analytical fervor yields fanciful results. In a simple mathematical model for estimating the likelihood of unauthorized disclosure of classified information, the probability of deliberate disclosure (PDD) is given as:

$$PDD = k_1 \times NP$$

where NP is the number of people who have access to the information and k_1 is "the disloyalty constant," i.e. the probability that one person will deliberately disclose the information. The value of k_1 is estimated to be around 10^{-5}, or one spy in each 100,000 cleared citizens, based on the record of detected espionage cases.

But experience indicates that "the disloyalty constant" is not a constant at all, nor is it strictly a function of loyalty. For one thing, with the uncontrolled expansion of government secrecy and the failure of declassification efforts to keep pace, more and more government officials are opting to covertly disclose ("leak") documents that are improperly classified. While they sometimes have personal axes to grind, they are hardly disloyal. Although the number of leakers exceeds the number of foreign spies by orders of magnitude, the proposed model arbitrarily excludes these deliberate disclosures. It might be noted that if the Clinton classification reform program fails to bring about decisive change, the public interest will increasingly depend upon this form of "disloyalty."

The 214 page report, the second of a projected four-volume series, is dated April 1993 and is available from the National Technical Information Service. It should be of interest to classification officials, cultural anthropologists, and the more desperate members of "the anti-secrecy underground."

Foreign Intelligence Surveillance

"The country doesn't give much of a shit about bugging," declared President Nixon in one of the newly disclosed Watergate tapes from 1972.

Be that as it may, the Foreign Intelligence Surveillance (FIS) Court maintained its spotless record by once again approving every application for surveillance put before it in 1992, according to the latest annual report to Congress.

Established by the Foreign Intelligence Surveillance Act (FISA) of 1978, this little-known federal court is empowered to authorize domestic surveillance of foreign powers or their agents (see S&GB 16). For security reasons, the FIS Court meets in secret and does not publish its rulings.

Electronic surveillance is undoubtedly an important counterintelligence tool. But the FIS Court's unvarying record of approvals suggests, at a minimum, that the system is not functioning as envisioned by Congress. Including the 484 applications approved by the FIS Court in 1992, a total of 7,045 surveillance applications have been approved since 1979. There have been no denials.

Meanwhile, the three-member FIS Appeals Court has become the Maytag repairman of the federal judiciary. Its services are never required since the lower court never issues any denials that could be subject to appeal.

Copies of all FISA Annual Reports since 1979 are available from our office.

Nuclear Rocket Terminated

In the classic science fiction melodrama "The Day the Earth Stood Still," alien emissary Michael Rennie ("Klatu") explains his mission to Earth as follows: "Soon your scientists will apply atomic energy to rocket flight. That will threaten the peace and security of other planets. That we cannot allow."

He needn't have worried.

The Space Nuclear Thermal Propulsion program, né Lofty Thunder, né Timberwind, has been cancelled by the Air Force due to funding constraints and the lack of an identified mission. (*Space News*, 5/17-23/93)

The unauthorized disclosure of the highly classified Timberwind program in 1991 is what gave the initial impetus to the current FAS project on government secrecy, since it seemed so clear that the program had been improperly classified as an unacknowledged special access program. This perception was confirmed late last year by the DOD Inspector General (S&GB 19).

Curiously, a senior official from Grumman Corp., a Timberwind contractor, told S&GB that whoever leaked Timberwind's existence did the program "a big favor," because it enabled the program to seek a broader constituency among other programs and agencies.

But the favor came too late, and the program was cancelled almost exactly twenty years after the cancellation of the last major U.S. nuclear rocket program (NERVA).

This repeated start-and-stop approach is obviously not the way to do business, and if human beings ever decide to boldly go where no one has gone before in outer space, they will still need to develop nuclear rocket propulsion. But not in secret.

* * *

The Secrecy & Government Bulletin is prepared by Steven Aftergood. Subscriptions are available from the Federation of American Scientists ($20 for 1993). The FAS Project on Secrecy & Government is supported by grants from the Rockefeller Family Fund, the J. Roderick MacArthur Foundation, the HKH Foundation, and the Millstream Fund.