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. 19
February 1993
ISSN 1061-0340

Eliminate Special Access Programs

Beyond the familiar classification levels of Confidential, Secret, and Top Secret, there is the special access classification system, which entails secrecy measures even more stringent-- and even more problematic-- than those of the regular classification system.

Agency heads are authorized by 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 ordinary (or "collateral") 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." (H. Rep. 102-60, p. 101). As part of a larger effort to restore some degree of propriety to the classification system and to cut unnecessary security costs, the Clinton Administration should act to eliminate the special access classification system.

Special Access Interview

It is in the nature of classified programs that their most pernicious practices are also the most insulated from criticism. In order to penetrate that barrier somewhat, S&GB editor Steven Aftergood met January 14 with a senior Pentagon security official (who requested anonymity) to discuss, in unclassified terms, the problems posed by special access programs.

S&GB: In your experience, have you found that the majority of special access programs (SAPs) are necessary or properly justified?

No. With a properly implemented collateral program [i.e. a regular classified program] with good, proper security measures, and the right need to know, you don't need a SAP.

Some people refer to SAPs as collateral programs with an access list. But it becomes much more than that, because they build up a lot of mystique about it. Senior people are usually kept in the dark about it, in the sense that they don't work it day to day. They are brought into certain rooms and briefed on it in a smoke and mirrors environment. They're scared. They're given the handshake. They're told only certain things, and they have other things to worry about, so they say OK, you take care of it. Once a year they get briefed on it, and the SAP people love that because they don't have any kind of accountability or oversight.

S&GB: What about other internal oversight?

In many cases SAPs were originally set up so they wouldn't be subject to review by the Defense Investigative Service (DIS). For years, DIS had almost no access to special access programs. For the last five years, there has been a concerted effort by DIS to get carved in [i.e. to be given oversight authority], because they were always carved out [i.e. not given access]. It was easy to carve them out.

I knew a lot of SAPs, where they used to brag about keeping DIS out. DIS would show up to a contractor [to do a security inspection], and the contractor would throw up a red flag and say, I'm sorry you can't go in that room-- that's a SAP room. DIS would get all pissed off, and there was a lot of friction. There was even guidance from the customer-- the government activity-- the customer says you can't go in there. The folks at DIS, through a lot of effort, have been able to get themselves involved in more programs, but still there's a lot of programs that they're carved out of.

Of course, what that does is, it eliminates independent oversight, at least from the security side, of the SAP.

S&GB: Is DIS really independent? They appear to be part of the DOD establishment.

You have to understand the SAP environment. There is a little group of people. They become very close. The contractors almost run most of them. In many cases it's sole source contracting. They'll write a contract that only one company can get. In the security area it's very specialized. There's a handful of companies around town, around the country that I know of that have exclusive rights. They in turn write the criteria and the government just nods, and they perpetuate their income from year to year. In the NRO [National Reconnaissance Office], for example, that's what happens there. It's a connivance between the contractors and the government activity.

But going to your question. DIS is independent. They're a separate agency. They're trustworthy, in my view. They should clearly have access and oversight for all agencies that are members of the National Industrial Security Program. But they were written out years ago. They supposedly weren't trustworthy. It was stupid. It was all part of this connivance between the contractor involved and that little program manager and his dollars. They are little fiefdoms and he becomes a god, if you will, with the contractors serving as his gofers. They do a lot of quasi-legal crap for him, because there is no oversight. It is a very shaky system.

The statement of work is usually tailored to the contractor so only that contractor can perform that work. They put a lot of unique requirements in there that could not withstand common sense scrutiny-- four inch doors instead of three inch doors, or whatever. They assumed the Soviets were on the other side of every wall in the country and built these expensive SCIFs [Sensitive Compartmented Information Facilities] out in the middle of the desert where the contract has to be performed.

S&GB: The procedure for briefing programs to senior officials or Congress seems inherently flawed, because the program is the only source of information, and the briefers only say what they want to say.

And there's very few questions.

S&GB: And there's very little basis to ask questions, because there's no independent source of information.

Exactly. I have some first hand knowledge of that-- I can't go into it with you-- but there are some flagrant violations.

What happens is that the security official involved buffaloes the agency heads, assistant secretaries, secretaries and says that's all you need to know. The people working the program know that they have to go see them at some point, so they tell them the minimum amount of information they can possibly get away with, and go off and do their own thing. And the programs take on a life of their own, and keep on eating up dollars.

The work itself may be good work, but a lot of money is wasted.

The abuse I've seen is primarily in the acquisition area. It's pretty well accepted in the security community that that's where it's been abused.

S&GB: Acquisition is one of the three SAP areas in DOD-- acquisition, intelligence, and operations, right?

Right.

S&GB: And acquisition means procurement, and research and development.

Yeah. Huge programs like the A-12 naval aircraft, the B-2 bomber, the F-117A stealth fighter all started out as SAP acquisition programs.

And the people that they brought in to supervise the security for those kind of programs came out of the intelligence area primarily, and they laid that [i.e. unique intelligence requirements] on acquisition. That's my experience. I've seen a lot of that. A contractor that has been working on a SAP gets a new customer and he wants to come into the same area and build another product. Then the new customer from the other agency comes in and says I'm sorry, although over the last ten years you did work here on a SAP for that customer, we're a new customer and those walls there-- we don't accept those. You have to tear down those walls and put up walls that are two inches thicker, or your door isn't wide enough, or the type of alarm system you have, or the clearances your people have, the investigations they're subject to, I'm sorry, they're now this plus a polygraph, or they have to go back seven years, or whatever....

The Presidential Directive recently to try to standardize the single scope background investigation-- the idea going in was a good idea, but it got muddied up and it's nowhere near what it should have been, because they still caveat it, allow exceptions.

S&GB: All these efforts towards simplification seem to get shipwrecked on SAPs, don't they?

Mm-hmm. The National Industrial Security Program [an attempt to streamline security regulations], for example, started out as a good idea. A lot of us thought it was a breath of fresh air. But it's been subverted by the SAP community. It's been made into a monster. SAPs have been its downfall, clear and simple. They've been allowed to steer the ship, they've been given way too much weight. I know of senior people who've tried to take them on, with some limited success, people within OSD [Office of the Secretary of Defense], people with good intentions. But the SAP people will pick up a phone and scare somebody at a very senior level, saying that if such-and-such changes are allowed to happen the world will come to an end, which is all nonsense. It's all nonsense. But people back off on them, they can't stand up to them.

If there was something like a NISP with a single, government-wide standard for investigations, for physical security, access control measures, etc., that would save the government millions and millions of dollars a year.

S&GB: The Aerospace Industries Association did an analysis which put annual industrial security costs at $13.8 billion in a single year.

And a large part of that is driven by the SAP community. When you start making security requirements more stringent [for SAPs], the vendors, the [security] contractors go nuts, they love it because it's a cash cow. And it just keeps coming and coming.

The way it is now, each SAP pretty much establishes its own security standards. Normally it is the contractor who writes it. The XYZ company, under contract, will write a security standard for this particular SAP at big bucks. And they will write the standard, in many cases, so that it is tailored to what they can provide. And then the program will turn right around and give that company a contract to provide the security services. And they'll say the individuals must have this kind of background, when the people who have that unique background are with that company.

In the [SAP] acquisition area, I saw them bring in stuff from the intelligence community that to me is ludicrous-- all kinds of phony phone numbers, mail drops, all kinds of stuff that, in my view, is way beyond rational requirements.

S&GB: What about other oversight?

Auditors, whether it's GAO, or agency or DOD auditors, often tend to be scared off. What I've seen happen is that an individual from the SAP will go to the head of the audit agency involved and say, we want to brief one of your people. They'll take someone who has very little background in security and they'll scare the shit out of him. They'll give him all kinds of magic briefings, bring him into the special room, ... all the hocus pocus. Then they can say, well, we've got an auditor involved. And if any questions come up on the program, they deal with that one auditor, and often, he's too intimidated to deal seriously with the issues.

S&GB: What about Congressional oversight of SAPs?

It's perfunctory. In my experience it's usually staffers, not Members, and it's a small cadre involved. And normally, I don't know, once a year or so, people will go up there and brief them on the particulars. Often it's several programs at one sitting. It's going through the motions.

S&GB: And this same cadre is presumably responsible for dozens, if not hundreds of SAPs.

Hundreds. They're really relying on the agencies involved to police themselves. Again, the way the structure is, that's difficult to do.

S&GB: The way the system is set up, it really discourages oversight, or renders it meaningless.

And anybody that tries to blow a whistle on it, of course, in the SAP area, it's the kiss of death. If you're working in that area and refuse to do anything, you'd be blackballed. Without any reason, they can pull an individual's access clearance. In that area, due process is not normally involved. Unlike the collateral area [the regular classification system], in my experience, where due process works pretty well.

S&GB: Again, Congressional oversight. You've done Congressional briefings on SAPs. Do they ask you good questions? Do they ask you any questions?

The ones I was involved with did not. They seemed to know what they wanted to know. They were going through the motions. There were one or two individuals that the program people that briefed were scared of, they were afraid of their questions, but overall it was a pretty friendly audience.

The people that are getting the briefings are powerful staffers because they have the yea or nay over funding for the programs, so they get stroked. They could for some unknown reason X-out that program.

They do get frustrated, you can see. You get comments to get DIS more involved, for example. But they're political animals, and they work for somebody, a Senator or Congressman, and those individuals have to be scared, if you will, of having their patriotism challenged by some group that's building a new weapons system, who will complain that Congressman so-and-so is questioning its value....

S&GB: A related factor is that in unacknowledged SAPs, you still can have contractors vigorously lobbying for their programs. Without challenge, or balance. In the Timberwind program, when it was still an unacknowledged SAP, contractors were lobbying for the program unopposed. In fact, I was told that several of the TW contracts were let with an eye on the contractors' geographical location and lobbying resources.

They become the biggest advocates of the program. The program manager may be a military officer and the program is his lifeline or his promotion. And he looks to the contractors to build support for the program. He often can't go to Congress directly. He has to go through the chain of command, but the contractors have a free hand.

S&GB: One of the things the recent GAO report seems to suggest is that the problem may be fixable on its own terms, by tighter controls, better reporting, etc.

I don't think it is. That's nibbling at the edges of the problem. I would challenge anybody in this day and age, and this environment, to explain why we would need a SAP to develop a new fighter plane, or a new ship, or tank, or whatever, if we had a decent collateral [regular classification] system....

S&GB: Aside from the excesses of the SAP system when it is functioning properly, or functioning the way it always does, is it your impression that the system promotes fraud or abuse?

I know of one case that I can't go into here. It's clearly, in my view, a very questionable program, that should not be in the SAP area at all.

S&GB: Was it put in the SAP area out of nefarious motives?

I wasn't there at the beginning. I think it was put in to make another agency happy.

S&GB: Is anybody looking at it, or is anybody even aware that there might be any impropriety?

No. The people running it have scared off the people that could put a stop to it. Very successfully.

S&GB: It's an acquisition program?

Mmmm.

S&GB: Is it reasonable to set as a goal the elimination of all SAPs, or all SAP acquisition programs?

It would be if you had a good, solid collateral program [i.e. a good regular classification system]. You couldn't do it in the existing environment because the collateral program is regarded as unreliable. The SAP community, they make jokes about the collateral people all the time, you know, that they're not trustworthy, etc.

Rather than fixing the problem, which is the collateral program, they create SAPs and SAPs-within-SAPs. If they went back and fixed the basic problem, which is the Executive Order [E.O. 12356 on classification], that's one thing, but it's a mindset. What you need to do is rebuild a new Executive Order, that has teeth in it, that's reasonable, that's based on a reasonable threat assessment. And then you need direction from the White House that this will be obeyed.

At the start, the new system should probably still allow for SAPs for operations and intelligence-- but not for acquisition-- with a goal of folding as many of those as possible into the new collateral program, once there's comfort that the collateral program is going to provide the protection that these programs warrant. It's all about enforcing need to know.

Both the SAP and the collateral worlds could be drastically reduced. I've seen thousands of classified documents in my time, and ninety percent of it all probably has no sensitivity whatsoever, much less does it threaten national security.

The point is the system is broke and they're not going to fix it without some leadership out of the White House.

S&GB: Couldn't the leadership come out of Congress?

No. Not on this issue. They're too political, they're too attuned. Contractors can get to them. In my view, the guy to do it is the National Security Adviser. Of course, he's got a lot of things on his plate.

Inspector General Audit on Timberwind

In an extraordinary new confirmation of what has become conventional wisdom, the DOD 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."

The 75 page report, initiated in response to a complaint by the Federation of American Scientists (FAS) in September 1991, 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 (NSIAD-93-78) looked at Timberwind but totally missed its improper classification, or the relation between excessive secrecy and the failure of the program.

A copy of the IG Report on Timberwind is available from our office.

National Industrial Security Program

The long anticipated, or dreaded, Executive Order authorizing the National Industrial Security Program was signed by President Bush on January 6 (E.O. 12829).

NISP began a few years ago as a well-founded effort to simplify the multifarious and conflicting security standards that industry is obliged to meet. According to the new Order, it "shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests."

There are at least two fundamental problems with it, however. First, it is rooted in the existing classification system which, as one NISP official put it, is "antiquated, if not corrupt." The original intent to combine NISP with new, less arbitrary classification criteria was abandoned by the Bush Administration as too politically sensitive.

The second problem is that, contrary to its basic premise, NISP is not "single, integrated, and cohesive." This important goal was derailed by the CIA and others who wanted to retain autonomous security authority. As a result, the NISP allows for unique requirements for "special classes of classified information," including Restricted Data, Sensitive Compartmented Information, and Special Access Program information, among others.

A new, 500 page draft of the NISP Operating Manual was completed in December 1992.

Overcoming Secrecy in Military Space

The outgoing National Space Council released a report January 4 that criticizes excessive secrecy in the highly classified world of military space and recommends that "the government seek to reduce, and where possible eliminate, security constraints associated with national security space programs."

The report of the Vice President's Space Policy Advisory Board, entitled "A Post Cold War Assessment of U.S. Space Policy," is all the more piquant because it is co-authored by legendary overclassifiers like Lt. Gen. James Abrahamson, who established Timberwind as a special access program in 1987.

"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," the report found. "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.... 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."

Therefore, "The President should establish policy guidance which limits the classification of all but the most sensitive technologies, systems, and information concerning space-related activities."

On January 11, Air Force Secretary Donald Rice announced a change in DOD policy "that will ease security restrictions on information about military space launches."

"When implemented, the change will mean that launch dates, payload data, and other associated information for most space launches will be declassified a reasonable period in advance." However, "Some launches involving classified payloads still require protection and will remain classified."

Last year, an Air Force launch that was secret in the U.S. was announced two days in advance by Tass radio in Moscow. (see S&GB 11).

Invention Secrecy Reform

The Pentagon is revising the standards by which secrecy orders are imposed on new inventions, following a flurry of protests last year about the explosive growth in new secrecy orders. (See S&GB 11, 12).

Since 1985, an increasing number of private inventors have been unable to get patents for their inventions in the U.S. because the Pentagon patent review board was imposing secrecy orders on unclassified, dual-use technology as a method of export control under the provisions of the Invention Secrecy Act of 1951.

From now on, the Defense Department will rely "primarily" on classification guides, rather than export control regulations, to determine whether invention secrecy is warranted. (*Federal Register*, 1/11/93, p. 3540).

DOE Classification Policy

The Department of Energy has completed a comprehensive assessment of the classification policies of the last 45 years as an initial step toward formulating changes in DOE classification policy.

The assessment is entitled "Classification Policy Study," and is dated July 4, 1992. DOE is withholding the document from release under the FOIA on grounds that it is predecisional, according to a 12 January denial letter from A. Bryan Siebert of DOE's Office of Classification.

"The 'Classification Policy Study' provides DOE comments and recommendations on possible changes to the DOE's classification program," Siebert wrote. "The views expressed in the document will be subject to consideration by the DOE and other agencies in the possible development of revised classification policies. The study is pre-decisional and is part of the deliberative process to develop revised classification policies and is, therefore, exempt from public disclosure."

DOE's refusal to release the document suggests that it might be moderately interesting. Rumor has it that the thrust of the proposed revisions would be to reorient classification practices along cost-benefit lines. Generally speaking, this seems to mean that efforts to protect certain information should be kept proportional to the damage, if any, that would result from disclosure. In other words, the recommendation is that DOE classification policy in the future should strive to achieve common sense.

Secret Poisoning of U.S. Veterans

In a grotesque and frightening abuse of authority, the U.S. government for decades concealed data from a series of tests in which American soldiers were exposed to toxic chemicals. Even today, several agencies are refusing to disclose their records of the tests while the survivors suffer a range of debilitating effects.

The tale is recounted in a new report by the prestigious Institute of Medicine (IOM), an arm of the National Academy of Sciences, released on January 6. The 425 page report, entitled "Veterans at Risk," attempts to identify the various diseases resulting from the tests for which veterans should now be entitled to seek compensation. The study was sponsored by the U.S. Department of Veteran Affairs.

In the course of World War II, some 60,000 U.S. servicemen were exposed to varying dosages of two chemical weapons, mustard gas and Lewisite, in preparation for their possible use in conflict. Though these weapons were never used, the tests were conducted in order to improve the weapons and the methods of protecting against them.

"The [IOM] committee discovered that an atmosphere of secrecy still exists to some extent regarding the WWII testing programs," the report found. "Although many documents pertaining to the WWII testing programs were declassified shortly after the war ended, others were not. Of those declassified, many remain 'restricted' to the present day and, therefore, not released to the public."

"This continuing secrecy, in the committee's view, has impeded well-informed health care for thousands of people."

* * *

The Secrecy & Government Bulletin is prepared and edited by Steven Aftergood. Subscriptions are available from the Federation of American Scientists at a cost of $20 per year. 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.