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. 25
August 1993
ISSN 1061-0340

## Prying Open the Intelligence Budget

Opponents of intelligence budget disclosure argue that acknowledging the overall intelligence budget number would inevitably lead to demand for more public information about individual agency budgets and programs, a demand that naturally must be nipped in the bud.

But that is all a charade. While officials pretend that the widely reported intelligence budget total is a secret, detailed information about individual agency budgets is already available or can be readily deduced if one knows where to look. So it is fortunate that, contrary to the assertions of some, the national security does not require concealing such information.

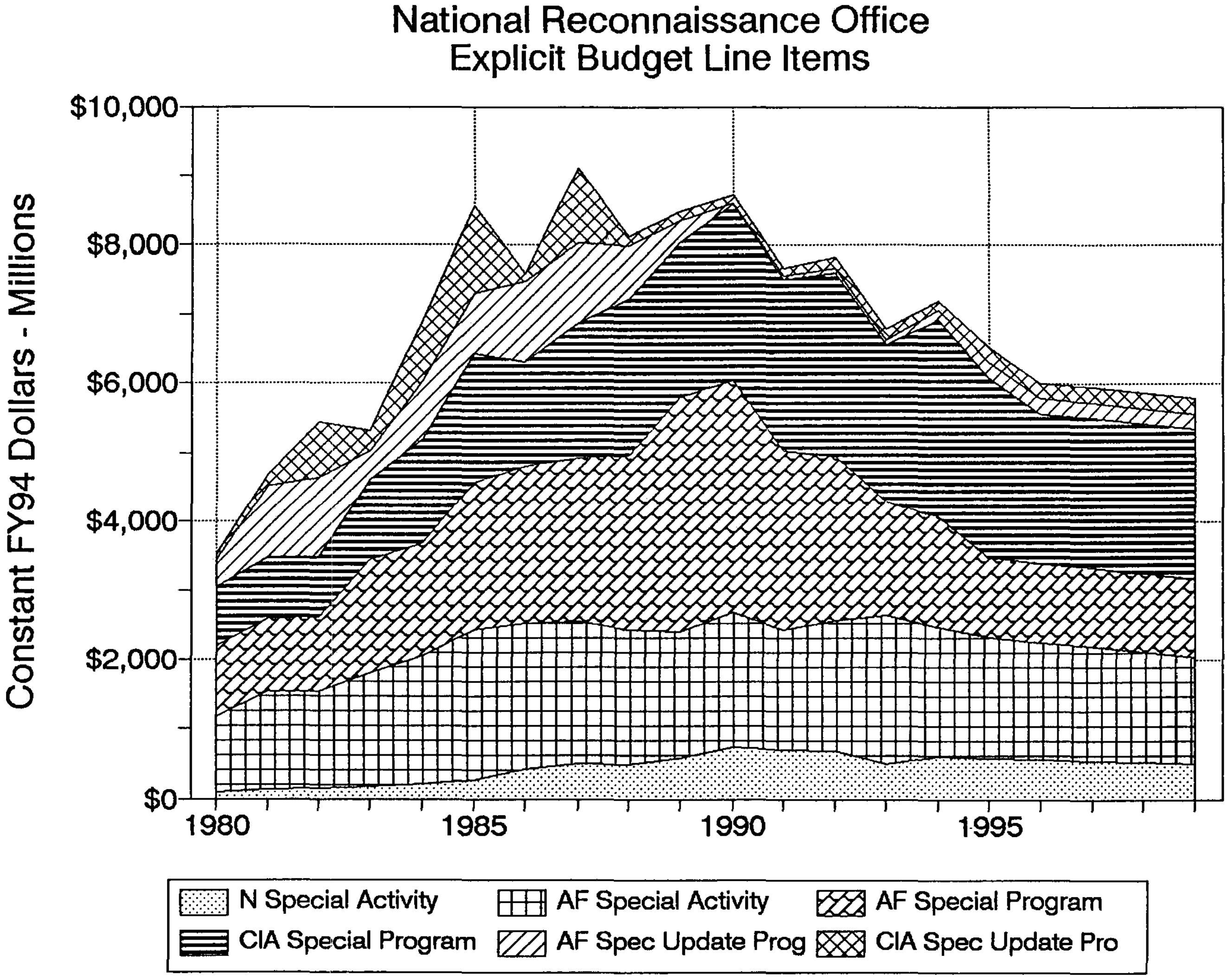
Below is a presentation of the budget of the National Reconnaissance Office, the DOD agency that procures and operates spy satellites and other reconnaissance systems. This budget estimate, from a report prepared by FAS space policy director John E. Pike, is derived primarily from a close reading of DOD budget documents, and some assiduous tracking of program element numbers. The estimate is based on unclassified documents up to the FY 1994 request and does not reflect ongoing budget actions in Congress.

Until its recent reorganization along functional lines (signals intelligence, imaging intelligence and ocean surveillance), the NRO was structured around its three executive agents-- the Navy, Air Force, and CIA.

Six corresponding line items in the defense budget contain the NRO budget. Navy Special Activities funds all aspects of the Navy's signals intelligence program. Air Force Special Activities funds research and development of other new intelligence satellites. The Air Force Special Program line item funds procurement of intelligence satellites assigned to the Air Force. The Special Programs line item in Other Procurement Air Force includes the entire CIA budget, as well as the CIA portion of the NRO satellite procurement budget that is presented below. Funding for launch vehicles for Air Force NRO programs is covered in the Air Force Special Update Program under Missile Procurement, while funding for launch vehicles for CIA NRO programs is covered under the Other Procurement Special Update program.

Further information and analysis is available in a new FAS report, "The NRO and NSA Budgets: Everything You Always Wanted to Know But Weren't Cleared to Ask."

Clearly, there are huge amounts of money at stake



in the NRO. In Congressional testimony last year, Gen. (ret.) William E. Odom complained that "'Success' for that agency [NRO] will be measured in how big a budget it can attain. Given a choice between two cheap systems and one expensive system, which will it prefer? The answer is two expensive systems."

But how expensive is an expensive spy satellite system? One reference point is the cost of Lockheed's Bus 1, the recently declassified spacecraft bus used on Keyhole reconnaissance satellites. According to the final report to the President on redesign of the space station, the cost of a naked Bus 1 exceeds $600 million. That would place the cost of an actual Keyhole satellite mounted on Bus 1 in the neighborhood of $2 billion apiece. To put that in some perspective, it means that the entire annual budget of the Central Intelligence Agency is the equivalent of about a satellite and a half.

### Classification Review Proceeds

The Presidential task force on classification reform is apparently sticking to its schedule, with an initial draft of a new Executive Order to be completed July 31. The next several months will be spent in revising and coordinating the draft prior to final submission to the National Security Council by November 30.

Will the draft text be made available at any point for public comment? "That's up to the White House," says Steve Garfinkel of the Information Security Oversight Office, who chairs the task force. But since lots of people are involved, and some of them are bound to be unhappy with whatever the task force draft ends up recommending, "We expect it to be leaked," he said.

The direction of the Clinton classification review process was also discussed in a keynote address to the National Classification Management Society on June 30 by Maynard C. Anderson. Mr. Anderson, who is among the more thoughtful and less dogmatic exponents of DOD security policy, is an Assistant Deputy Secretary of Defense, with responsibility for International Security Programs, special access programs, and foreign disclosure policy. Excerpts from his remarks follow.

"I anticipate that the national security information review will result in more than perfunctory tinkering with the system. I expect that it will examine the categories that need protection, with a view toward identifying those that may be declassified in bulk, in a 'Cold War is over' approach."

"This review should result in means of enforcement, not merely measurement, of the program's effectiveness. And its effectiveness has to be how well it protects information and how well it protects the public's interest."

"The program effectiveness must include an evaluation of the propriety of classification actions. I would like to see some emphasis shifted from the controls on classified information to controls on classification actions. Penalties for unauthorized disclosure of classified information should be accompanied by penalties for improper application of classification. I believe this might be one way to remove the long term undesirable consequences of unnecessary protection of information."

"Classifications are arbitrary, artificial designations of information sensitivity devised by program managers and often, I fear, to satisfy their desires for exclusivity."

"There are legitimate reasons for protection of information: to preserve human life directly or indirectly by protection of operations, intelligence sources and methods, or advanced systems and countermeasures. There are not many justifications for imposition of severe constraints on information distribution beyond those."

"The review should mandate new standards for the establishment of special access programs, allowing them to be created only when the information cannot be protected by the most stringent means [available in the regular classification system] except in rare situations where a person's life is in danger or the national security would be irreparably jeopardized by a lower standard of protection."

"If the need for protection of classified information were allowed to seek its own level in response to the risk of compromise through faulty physical security measures, it is doubtful that it would exceed the requirements for commercial insurance coverage on most of our property."

### Contractor Document Destruction

The preservation of a large quantity of classified documents of historical or technical value held by government contractors may be jeopardized due to irresponsible document handling procedures and even willful destruction.

"Important pieces of the history of military contracting and contractors have already been lost or are endangered," according to the recently released proceedings of a November 1992 conference on "Preserving the History of the Military Contracting Industry." The conference, held at the Rand Corporation, was co-sponsored by the Department of Defense, the National Archives, and the Smithsonian Institution.

"In reaction to the ever-present threat [sic] of public disclosure through FOIA, some in the higher echelons of Federal agencies avoid keeping records," one academic participant stated. "Although many records cannot be found in Government offices,... they are often located in contractor files. This situation makes the preservation of contractor records all the more essential."

In a roundtable discussion, "Many participants noted the disturbing trend of destruction of classified material in contractor archives. [One participant] noted her experience in which there was a pervasive perception that DOD wanted records destroyed, and many participants concurred. [She] explained that DOD has a continuing right to inspect any facility that holds classified material, a situation that often motivates the removal or destruction of such material."

"[A representative of] Aerospace Corporation said his corporate security department actively tells employees to destroy every classified document possible, irrespective of content." Another participant responded that, in theory, "Federal records cannot legally be thrown away without approved disposition authority."

However, according to a September 1992 DOD handbook on document destruction, "Anyone who is authorized access to the classified materials is allowed to destroy those materials without being appointed as a destruction official." Further, "If you have no operational need to retain a classified document and if there is no historical value to the document, you should promptly and properly destroy the document."

But how do you determine if a document has historical value? "Check with your records management office."

On the practical side, "DOD recommends that you do not shred just one sheet of paper containing classified information and subsequently leave it in the shred bag. You should shred other similar (in color and print text) sheets of paper (classified or unclassified) so the shredded pieces will be mingled. This will make it extremely difficult, if not impossible, for someone to reconstruct the classified sheet of paper. A good rule of thumb is to shred and mix at least twenty sheets of paper."

*Copies of the conference proceedings and the DOD handbook are available from our office.*

* * *

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. This publication may be freely reproduced.

## SAPs, RAPs, and Other... Stuff

The idea that government activities, such as law enforcement, for example, must function within certain externally imposed norms is not widely understood or accepted in the bowels of the national security bureaucracy where highly classified special access programs flourish. Nominal standards are disregarded and new procedures are secretly invented to serve the narrowest interests of individual program managers. It's as if some new form of government were gestating beyond the scope of permissible public awareness where the usual rules just don't apply.

A glimpse of the Defense Department's difficulties in controlling the proliferation of autonomous secret programs was provided at a panel on special access programs (SAPs) at a meeting of the National Classification Management Society in Atlantic City on June 30. Excerpts are presented below.

The panelists cited here are **David Whitman**, a deputy director for security classification and safeguards in the Office of the Secretary of Defense, and **Richard Williams**, assistant for special programs in the Office of the Deputy Under Secretary of Defense. Some of the views presented are arguable, misleading, or simply wrong. Caveat lector.

* * *

**Question: Why isn't there sufficient confidence in the regular classification system so that SAPs are not needed?**

**David Whitman:** I'm not certain that there is a positive answer. I guess it boils down to a lack of discipline in the application of need to know. Occasionally we see evidence in some quarters that there's almost no need to know and that's very disturbing. And in other cases it's a little bit slipshod. It leads me to conclude that there have got to be program managers out there who just feel an absolute need to control who gets the information. And if they feel that way because need to know is poorly implemented, that's the driver to a great many of our SAPs.

I would add that in the work of the [Clinton Administration] PRD 29 Task Force [on classification reform], at least two of the committees have concluded that one of the fixes to this problem-- and I consider SAPs a problem, because I believe there are too many of them-- one of the keys to fixing it is to take a tool from the SAP world that can help and to place that tool in the normal world of security tools-- and I'm referring simply to an access list. Let an access list be part of the normal world and with some controls at fairly senior levels, allow managers to implement that tool in the normal security world.

**Richard Williams:** Having a classified document years ago was something really special. And then a lot of people started classifying things, and they classified everything. Why? The reason in my opinion is because you couldn't keep it out of the public domain. In other words, the Freedom of Information Act would cause the release to the Bulgarian Library Service or whoever immediately after you released it. And therefore people started to classify [more]....

Now as you started to classify everything, it became necessary to call out those things that are most important, that really required additional security protective controls. And that's the first part of my answer to the question [of why SAPs were needed].

The second part [of the answer] is the cost. Essentially we dedicated the resources and the efforts into protecting those things that were called out as SAPs. We spent the money to protect them and we did protect them. There's a few that have been lost along the way but generally these programs have been very well protected. You see this in the way that they get to production and into the field without really being compromised. There's no countermeasures.

As you put things side by side-- an example might be, for the sake of discussion, the B-1 bomber versus the [Soviet] Blackjack bomber, as opposed to say the F117A. Where's the companion? There isn't one. Why isn't there one? Because we protected it.

Therefore, senior policy makers-- because they're the ones that make the decisions on what would and wouldn't be special access-- decided they needed to call these programs out and put additional protective measures in there. And the seedbed of discontent that caused that, in my opinion, is that everything became classified, because we had no other vehicle to protect it from public domain.

Now, what's wrong with the regular system? First of all, we have uneducated people-- I'm talking generically-- making classification decisions. We had some very good training aids we put together, and we caused people to look at them, but somehow the message just didn't get through to the degree we wanted.

Dave has suggested perhaps taking from the special access world the idea of using an access list. I don't disagree with that in principle, however in practice it becomes a problem. Because just a short way from extracting and making an access list is additional vetting, and just shortly behind that is additional protective measures, and shortly behind that is computerizing that access list, and as soon as you start to employ these kinds of measures, unless you very rigidly control them, what you have essentially is a programmatic approach to security, which constitutes a special access program, whether you call it one and identify it as one, or not.

Many of you have been exposed to programs that were not called special access programs, but by criteria they certainly were SAPs. It's a foundational question. Is a SAP a program that an agency head signs off on as a SAP, or is a SAP one that has the criteria applications of something beyond what's normal? And that becomes a foundational question when you start trying to control these programs with additional protective measures.

**Q. Will the designator LIMDIS ["limited distribution"] be eliminated and, if so, will we lose the line separating normal programs from SAPs?**

**Dave Whitman:** I'd like to try to answer the last part of the question first. Elimination of LIMDIS would sharply clarify the line between SAPs and the normal world. Right now, in my estimate, LIMDIS blurs that line. It's a transition that's very gray, not well understood even in the DOD world. And keep in mind that it's a DOD creation, although even in the DOD world it is practiced only in a few agencies.

You may recall that we had legislation last year [see S&GB 15] that required our reporting certain financial information and other data concerning so-called "LIMDIS programs."

Only about 80 such animals were reported-- Navy, Air Force, Defense Nuclear Agency, and the Advanced Research Projects Agency were the contributors. And within those four DOD components, the number of programs with LIMDIS information was dropping rapidly because of all the grief caused by the reporting requirement, and a realization that perhaps it wasn't buying much. The Defense Intelligence Agency probably has another dozen of those things which were not required to be reported-- there was a small exception for them built into the legislation. So perhaps 95 or so LIMDIS-like things within DOD. Not many, when you consider everything.

Will LIMDIS be eliminated? I think now we have a better chance of eliminating it than previously. I think LIMDIS will be eliminated, and I think now that the thing that will do it for us is moving that tool from the special access world to the normal world that I referred to as an access list.

**Dick Williams:** Whether you have LIMDIS or not is really of no consequence.

Why do we have LIMDIS? Well, Maynard [Anderson] asked the contractors, once upon a time, do you have [specially controlled] programs that are other than special access programs? And I think they identified about 450 programs that were other kinds of programs that were not

SAPs where they had to do exotic types of security procedures.

But when you go through and look at the breakout, at what point do you draw the line [between normal programs and SAPs]? And the General Accounting Office told us we need to do a better job of drawing that line. As a matter of fact, they said that we had one agency that had 1600 programs that were not SAPs and were not normal.

So how do you draw the line? What kind of criteria do you put in place and say, if you cross over this line you are in fact a special access program?

Or do you just solve the problem this way, and incidentally this is a real easy way to solve the problem: We won't have any more SAPs-- you can do whatever you want to do and call it normal. It's real easy. We can sign that out tomorrow, solve the problem. We won't have any more SAPs and you can do whatever you want and call it normal.

Does everybody see the problem here? The problem is, how do you identify where that line is? Is it additional vetting of clearances? Is it control of need to know? Is it the physical security upgrades?

The question that I have for you, and I don't think there's a ready answer for this, is how do you want to identify when you make the transition from what's normal to what is in fact not normal and is going to be protected with extraordinary means?

How do we make these policies very clear? We chose to do it on an interim basis using LIMDIS. Because if you really want to control it, you've got to first of all identify when you make the transition. So this was our fledgling first attempt to try to draw that line very clearly. And if you go beyond those things-- essentially certain types of physical controls, information and personnel security controls-- then, by definition, by criteria, you become a SAP.

Now we can move that list back, and say anything's normal. There's got to be a very clear definition of what's normal. Because if not, you'll have programs that were the same type as, if you read your history, Sun Tzu described as special access programs, because the reason for these kinds of programs is compelling.

You're not going to eliminate the basic behavioral trait that when you have something you want to protect, and you've decided to protect it, you're going to put extraordinary measures in there to protect it. All you're doing is setting an artificial line and the question is how and where do you want to put the line.

So eliminating LIMDIS is not the problem; establishing the line is the problem.

How many of you have heard of RAPs? Who knows what a RAP is? It's a Restricted Access Program [*a bogus designation devised to evade controls on special access programs*]. There were over a thousand of those. We eliminated them.

The point I'm making to you is you've got to figure out how to draw that line so that you eliminate the ones that do not have proper approval and in fact are operating beyond the normal range.

Some of you know exactly what these different kinds of designators are. "Must Know" [*another bogus control on access*]-- have you ever heard that term? Most of you have heard that term. And this is the problem we're trying to deal with.

**Dave Whitman**: One of the committees of the PRD 29 Task Force is looking at SAPs and has evolved a starkly different definition of what a SAP would be. And as I recall it, and it's a moving target now, and it's only a proposition, a SAP would become a program that employed enhanced personnel and adjudication criteria and nothing else.

A couple of the Committees on the Task Force have come to the conclusion that the new replacement Executive Order ought to say that if it's not provided for in this Order, You shall not do it. And that then becomes an Order from the Commander in Chief, the President of the United States. That may bring some discipline and help avoid things like the thousand RAPs and the other ingenious little devices that in the end wind up causing great consternation.

**Dick Williams**: Let's take that as an example. Say we eliminate everything but physical security and personnel security. Having been a senior program manager, what would I require you to do? Keep detailed listings of everybody that had seen the information, have that centrally programmed, I would check the computer system to make sure you were doing it properly, have you inventory it weekly... Is everybody getting the picture here? Once you allow the latitude in, the question is how much latitude are you going to allow? You know as well as I do having dealt with government customers, they can come up with very inventive ways to have you control the information.

So when you forge the definition, if you allow that kind of opening-- essentially information security is not covered only personnel and physical and maybe technical-- then you've opened up a whole new avenue of opportunity for senior program managers to do what they think's best. And you've got to be very careful when you establish that because once you open that up you have to face the consequences of that action, of putting that policy in place.

**Dave Whitman**: I may have misspoken. What I was suggesting was that the Order would come out prohibiting any such creativity.

**Dick Williams**: The problem that I see there-- it would be like trying to impose gun registration. You don't want to drive everybody underground.

So you're better off to have the rules well established and have them out in the open than you are to force people to do the kinds of things they have to to protect the programs.

You've heard this said from the Office of Policy many times. The policy has got to be workable. It's got to be almost easier for the person to do the right thing than it is to do the wrong thing. Because if you make that policy unworkable, senior program managers will find out ways to make that policy work the way they want it to....

Certainly for a long time we have not done a very good job of reconciling the different issues between the intelligence community and the collateral community.

Let me give you a specific example. There must be thinner people, people who don't weigh as much, working in the intelligence community. How do I know that? Because on physical security [for portals and ducts], they protect against [openings of] 90 square inches and the collateral side protects against 96 square inches. ˜So my conclusion is that there would have to be, by necessity, thinner people working in the intelligence community.

[The system is] filled with these [kinds of inconsistencies]... Under the Industrial Security Program they use the UL system. Why? Because the first alarm systems burned the buildings down so they had to have safety requirements. But in the intelligence community for years they used specialized alarm provisions, no UL provisions. And I could go down the line, whether you're talking about vetting clearances or information security techniques...

We don't need documents that have skinny people in one program and heavy people in one program. I mean, we just don't need to do that. We need to do this intelligently, and do it correctly, and there's certainly a foundational reason for having the National Industrial Security Program, and that is to try to put these procedures into some type of logical constructive order.

**Maynard Anderson**: The discipline has to start with the predicating action of classification. If you do not start there, and if you do not penalize for excess or indiscriminate or superfluous or foolish or stupid classification, then all of this other stuff is immaterial.

**Dick Williams**: Seems I saw you on a tape saying that same thing.

**Maynard Anderson**: Seems you probably did. And you didn't pay a damn bit of attention then either.