

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. 13  
August 1992  
ISSN 1061-0340

### Cover Stories

"There are standards in villainy as in virtue," wrote Joseph Conrad. The Defense Department authorizes its contractors to deceive the public about the character and existence of certain secret military programs, as long as they do it believably.

"Cover stories may be established for unacknowledged programs in order to protect the integrity of the program from individuals who do not have a need to know. Cover stories must be believable and cannot reveal any information regarding the true nature of the contract." (from Special Access Program Supplement to the National Industrial Security Program Manual, draft 29 May 92, section 3-100(n), For Official Use Only).

The premise here is that Defense Department "black" programs are so sensitive that their very existence (not just the details of genuinely sensitive technologies) must be concealed from the public. And to effect that concealment, mere secrecy is sometimes not enough-- false information, or cover stories, may have to be actively circulated. This kind of policy implicitly casts a shade of doubt on all public statements issued by the Defense Department.

A new Defense Department Report to Congress on the Management of Special Access Programs warns against Congressional initiatives like establishing a fiscal threshold above which a program could not remain "black." The Pentagon promises (for the umpteenth time now) improved oversight of highly secret special access programs. "The procedures now being implemented within the Department... will achieve more effective oversight and control of special access programs." It's believable.

### National Industrial Security Program

In its way, U.S. industry is as much a victim of excessive government secrecy as anyone else, since it is industry that actually has to implement much of the convoluted security policy prescribed by the government.

The new National Industrial Security Program (NISP), intended to mitigate some of industry's concerns, is shaping up to become the most important innovation in the handling of classified information in more than a decade. But it's a mess.

The motivation for the NISP is perfectly reasonable. There are dozens of different, and conflicting, standards and guidelines for safeguarding classified information. Complying with all of them is either very expensive or impossible. "Well-intended security programs have become so divergent as to seriously erode our effectiveness in carrying them out," according to Ron Beatty, Director of Security at Rockwell International.

NISP is an attempt to streamline the system by generating a single, integrated government-wide standard for protecting classified information. But the monstrous initial draft of the NISP Operating Manual (5 June 92)

doesn't quite fit the bill. It consolidates many of the different standards in one huge volume, but without truly integrating them. Thus, in addition to the "baseline" standard, there still remain different supplemental standards for special access programs, sensitive compartmented information, communications security, etc.

The NISP was developed by defense contractors in partnership with executive branch agencies (DOD, CIA, DOE). But even within this military-industrial axis, it has been necessary to suppress dissenting views. The National Security Council advised the participants that "President Bush wants a NISP" and that free-thinkers and foot-draggers would be reported to General Scowcroft, a fearful prospect.

One of the current disputes concerns the handling of information classified Secret. Industry has recommended eliminating the requirement for strict accountability (recording receipt, source, ID number, disposition, etc.) of Secret material. Industry spokesmen argue that government doesn't impose this accountability requirement on itself, so why should they have to put up with it? Others within the NISP program say "this change may have a profound and unanticipated negative impact."

In another disputed action, one confused NISP working group recommended imposing program-specific security requirements on special access programs. But as noted in the cover letter transmitting the NISPOM draft, "This recommendation is inconsistent with the concept of the NISP and, in fact, perpetuates the very problem that was a major impetus for the development of a NISP."

The initial draft of the NISP Operating Manual is circulating among the participants for comment until September 1. A revised draft will be issued in January for wider distribution. The NISPOM would not officially take effect until one year after issuance of the forthcoming Executive Order authorizing the NISP.

### More Secrecy Needed

"There's a lot of information that's classified that's not as sensitive as some that's unclassified," declared Information Security Oversight Office Director Steve Garfinkel at a National Classification Management Society panel in Dallas on July 1.

The conclusion Garfinkel draws from this fact, however, was not that a lot of classified information should be immediately declassified. Instead, he argued, more restrictions will be needed on *unclassified* information! "I think ultimately we have no choice but to tear down the rather artificial barrier between the classified world and the unclassified world."

But "if we are going to go beyond the classified world to sensitive unclassified information of various sorts, we're going to get into the realm of a number of different statutes, and we're going to necessarily involve the Congress very much in the process." And since cooperation with the legislative branch "is not currently at

its all time optimal level,... I just don't see it happening in the near term."

#### New Executive Order on Classification Delayed

Garfinkel went on to say that "We are going to have revisions to Executive Order 12356 [the 1982 Reagan order on classification], and I believe those revisions will come about next year."

Earlier, this new Executive Order replacing 12356 was expected to be linked with an Order authorizing the new National Industrial Security Program. "They're no longer linked," said Garfinkel. "But I'm not going to tell you why they're no longer linked." Others explain that the new Order on classification was separated off because it was deemed too sensitive for an election year. The Bush Administration does not want classification and government secrecy to become campaign issues.

But the new Order on classification "is going to be back on schedule in terms of the creation of a working draft, I would say, early next year." The specter haunting all of this activity, including the NISP, is the unspoken fear of a change of Administration next year, which could make much of this work moot.

#### A CIA Move Toward Increased Openness

In a welcome, if modest, gesture toward greater openness at the Central Intelligence Agency, Director Robert Gates on April 28 approved a new internal regulation on Information and Records Management that prescribes guidelines for declassification of historical CIA records, mainly those thirty years old or older.

Notably, the regulation establishes a systematic declassification review process (to exclude certain operational files) and states that "there shall be a presumption in favor of disclosure," again with certain exceptions.

Although the Reagan Executive Order *presumes* that disclosure of foreign government information, the identity of a confidential foreign source, and intelligence sources and methods would all cause damage to the national security, the new regulation states that "such information shall not be automatically withheld under this Program, but must be reviewed for possible declassification even if it concerns matters normally withheld from public release."

In language that harks back to the more progressive standards of the Carter era, the regulation directs that "Reviewers... who advocate the continued classification of information will bear the burden of identifying any damage its disclosure reasonably could be expected to cause to the national security. Information... may remain classified only if the reviewer can identify such damage and a clear connection between disclosure and the projected damage."

*A copy of the new CIA regulation may be obtained from our office.*

#### CIA Document Destruction

By letter of 29 June, the CIA took the trouble to deny our assertion (see last issue) that it destroys official documents secretly. "By law, this Agency may destroy Federal records only with the approval of the National Archives and Records Administration and in accordance with established procedures (44 U.S.C. 3314)." In other words, CIA is complying with the law, and the government documents it destroys are not kept secret from the Archivist.

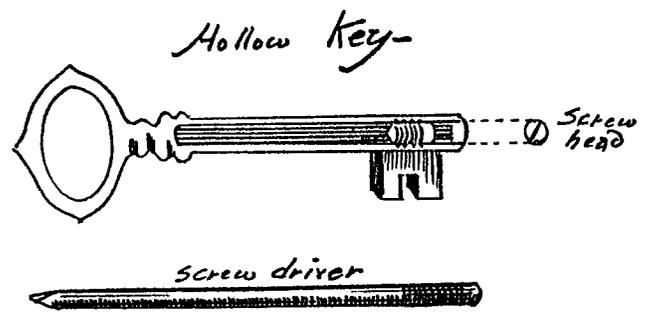
The fact remains, however, that the document destruction proposals (not just the documents themselves) are classified by the CIA and unavailable to the public. Archives officials insist they are particularly vigilant in reviewing CIA document destruction and, in all probability, the affected documents really are worthless. But it is unclear why an unclassified description of this irreversible action cannot be prepared.

#### Now It Can Be Told

On June 3, the Secretary of the Army went out on a limb and authorized the declassification of a World War I report that we had requested last fall. Dated April 15, 1917, it had been identified by officials at the National Archives as among the oldest classified military documents in their holdings. During its last classification review in 1976, the report-- entitled "On the Intelligence System Necessary in Case U.S. Troops are Ordered to the Continent"-- was exempted from automatic declassification.

We could not find anyone willing to defend the 75 year long suppression of this document-- even Steve Garfinkel said "it seems absurd"-- but for some time it probably remained classified because it names some individuals who assisted the intelligence effort in WWI.

An engaging first person narrative, the report begins: "On February 1, as there seemed to me a possibility of the U.S. becoming seriously involved in this war, I began figuring on the consequences resulting if our troops were sent abroad to cooperate with the allies." Along with plenty of inane commentary ("We have to control our expenses in Holland") and information on the "techniques" of train watching, some vintage intelligence sources and methods are disclosed, like this diagram of a hollow key for transporting secret messages:



The text 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."

#### Miscellany

- Contractors to the National Security Agency are advised that, "If you are asked about the activities of NSA, the best response is 'no comment.' You should then notify your [security officer] of the attempted inquiry."
- According to NSA internal regulations, employees and contractors are "discouraged" from using the terms Signals Intelligence, Communications Intelligence, and Electronic Intelligence "in a public forum."
- A questionable new NSA "security education" poster features the face of a black man with the caption "Bo Has No Need to Know." A Defense Department spokesman said the poster is "absolutely not" racist and merely plays off the "Bo Knows" advertising campaign.
- In a special edition of Current News, an anthology of news clippings on Equal Opportunity and minority issues, the Pentagon mistakenly included an *Aerospace Daily* story about special access or "black" programs.
- A recent Energy Department directive on "Foreign Travel Authorization" lists Andorra, the tiny nation lodged between France and Spain, as a "sensitive" country.
- Certain classified programs are required to have a secret, non-attributable telephone number, known as a Hello Line. "When answering a non-attributable telephone, program personnel will state the proper salutation, e.g. Good Morning or Hello. Do not use the company name."

\* \* \*

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 (about 10 issues). The FAS Project on Secrecy & Government is supported by grants from the Rockefeller Family Fund and the J. Roderick MacArthur Foundation.