Coming: The Big Chill?

Not content that the current system of counterespionage and export controls is adequately safeguarding scientific and technical data, the Reagan administration has been experimenting with additional programs — some that risk straining the bounds of legality

By JANET RALOFF

For years, the Reagan administration has been stepping up its campaign to counter foreign espionage. These efforts have tended to focus on increased surveillance and prosecution of suspected spies and on a strengthening of national security controls affecting the "export" of technologies believed to be militarily critical. But several measures launched quietly over the past year go beyond these. In the view of some, they threaten to overstep the statutory powers of the United States' national security agencies.

Among the measures in question:

• the recent visits to commercial database vendors by teams of national security officials. The stated intent of the visits – which were widely viewed by the recipients as "intimidating" – was to suggest that these private businesses begin voluntarily restricting the unclassified data (including newspaper articles, publicly released government reports and congressional-hearings transcripts) they sell to foreign subscribers.

• a new Department of Energy (DOE) program aimed at discouraging scientists at national laboratories from sharing unclassified research data.

• the recent revelation that NASA has compiled what it calls a "No-No List" aimed at preventing people involved in foreign technology-exchange programs, including U.S. academics, from subscribing to an unclassified federal publication. While the list may not be new to this administration, it only came to light in the past few months and is a reflection of current administration policy.

An illustration used in a campaign to promote LLNL-employee awareness of the lab's SAFE program.

One thing these programs share is the potential to impose a "chilling effect" on the free flow of nonclassified scientific information, says Robert L. Park, executive director of the American Physical Society's public affairs office. Park is a leading critic of government controls on nonclassified data. Not only does he question the utility of such controls in keeping new technologies out of the hands of the Warsaw Pact, but he also sees them threatening "to hold back our own [U.S.] research program."

"To a very large extent," says Park, "the workforce we'll be keeping ignorant will be our own."

One of the new programs to slow the flow of U.S. technical data to the Soviets is known as SAFE – Security Awareness For Employees. Launched at Lawrence Livermore National Laboratory (LLNL) in Livermore, Calif., last year by the Department of Energy, it's the prototype for a program that is expected ultimately to be implemented throughout the rest of DOE's laboratories and contractors. SAFE not only aims to acquaint laboratory scientists with the notion that they may inadvertently become the targets of potential recruitment by Soviet agents, but also teaches them how foreign spies operate, what they want and how they can be foiled.

To bring home the message, the program provides video presentations, such

as "The KGB and You," and talks by such guest speakers as a Soviet defector and the director of intelligence and counterintelligence for the National Security Council.

According to a staff announcement on the program circulated among lab managers last year, "The insider threat is defined as something an employee may do, either wittingly or unwittingly, to jeopardize the laboratory and national security. This threat runs the gamut from deliberately selling or giving away classified information to innocently providing unclassified information which may complete a part of a classified puzzle." (Livermore officials refused to discuss the program with SCIENCE NEWS.)

There's also another goal, one not stated in the official handouts. As explained to SCIENCE NEWS by Edward V. Badolato, then assistant secretary for security affairs at DOE and one of the designers of the SAFE program, "We want to put the fear of God in them [DOE scientists]." Talking informally after a Heritage Foundation seminar in Washington, D.C., on the use of Soviet scientists for information gathering, Badolato voiced concern about what he sees as the dangerous naiveté of U.S. scientists in dealing with Eastern Bloc colleagues.

Many DOE scientists, he says, don't seem to know whether their unclassified work is subject to export controls, and so they might accidentally reveal too much to a foreign colleague during casual conversation. With DOE's stepped-up security awareness program, he says, scientists would be informed that such ignorance would not protect them against felony prosecution if they were caught. This knowledge should make them think before they talk, and should curtail discussion of many of the research details they might otherwise openly share with friend and foe alike, Badolato says.

If the scientists encouraged to participate in this program were only those whose work is classified, or unclassified but subject to export controls (SN: 1/24/87, p.55), then DOE's SAFE program might prove both educational and beneficial, says Park. But, he charges, if the SAFE program includes lab personnel whose work is not subject to censoring controls, then it risks "imposing on them a chilling effect" with regard to the normal free flow of scientific information. One national security official at DOE told SCIENCE NEWS that this program is widely directed to all DOE lab personnel.

Even among scientists whose work is subject to export controls, Park says, it behooves DOE to alert them to that fact and to tell them why their work is controlled—neither of which the agency now does.

But Sid Stembridge, who coordinated LLNL's SAFE program until his retirement last March, has justified the program, saying, "We do know that [LLNL] has been 'targeted' by certain foreign intelligence agencies. We do know that a number of employees and contract workers have been approached. And the DOE assumes, for planning purposes, that each DOE facility has at least one insider [internal spy]." Stembridge's remarks were printed in MANAGEMENT NEWS NOTES, an internal LLNL publication. He declined to be interviewed by SCIENCE NEWS on the SAFE program. DOE also has declined to offer additional information about the extent of spying at its facilities, including LLNL, or to furnish the names of any employees approached by foreign agents.

"We do know that [LLNL] has been 'targeted' by certain foreign intelligence agencies. . . . DOE assumes, for planning purposes, that each DOE facility has at least one insider [internal spy]."

The SAFE program is not very visible outside LLNL. But some who have heard of it are concerned about its potential for encouraging more self-censorship than national security laws require. In fact, Park maintains, "I think they [DOE] have used uncertainty all along as a kind of weapon" — to pose not only the implied threat of possible legal action, but also the implied threat that a scientist's research contracts through the agency might not be renewed. For this reason, he sees DOE's SAFE program as potentially ripe for abuse by the administration's national security apparatus. Regarding Park's comments, an official of DOE's defense programs office — which oversees the SAFE program — told SCIENCE NEWS, "it's not appropriate for us to give you a comment."

Another recent administration initiative responsible for sending shivers through much of the commercial data industry came to light as national security officials began visiting private business leaders to propose new restrictions on the commercial packaging and sale of nonclassified information.

Jack W. Simpson, president of the Dayton, Ohio-based Mead Data Central, learned of the proposal last year through "suggestions" made to him during four visits by members of the Department of Defense, Federal Bureau of Investigation, Central Intelligence Agency and National Security Agency. At an Information Industry Association meeting last November, he described these "friendly" meetings as "involving only suggestions and questions. But their ultimate intent," he said, "is absolutely chilling."

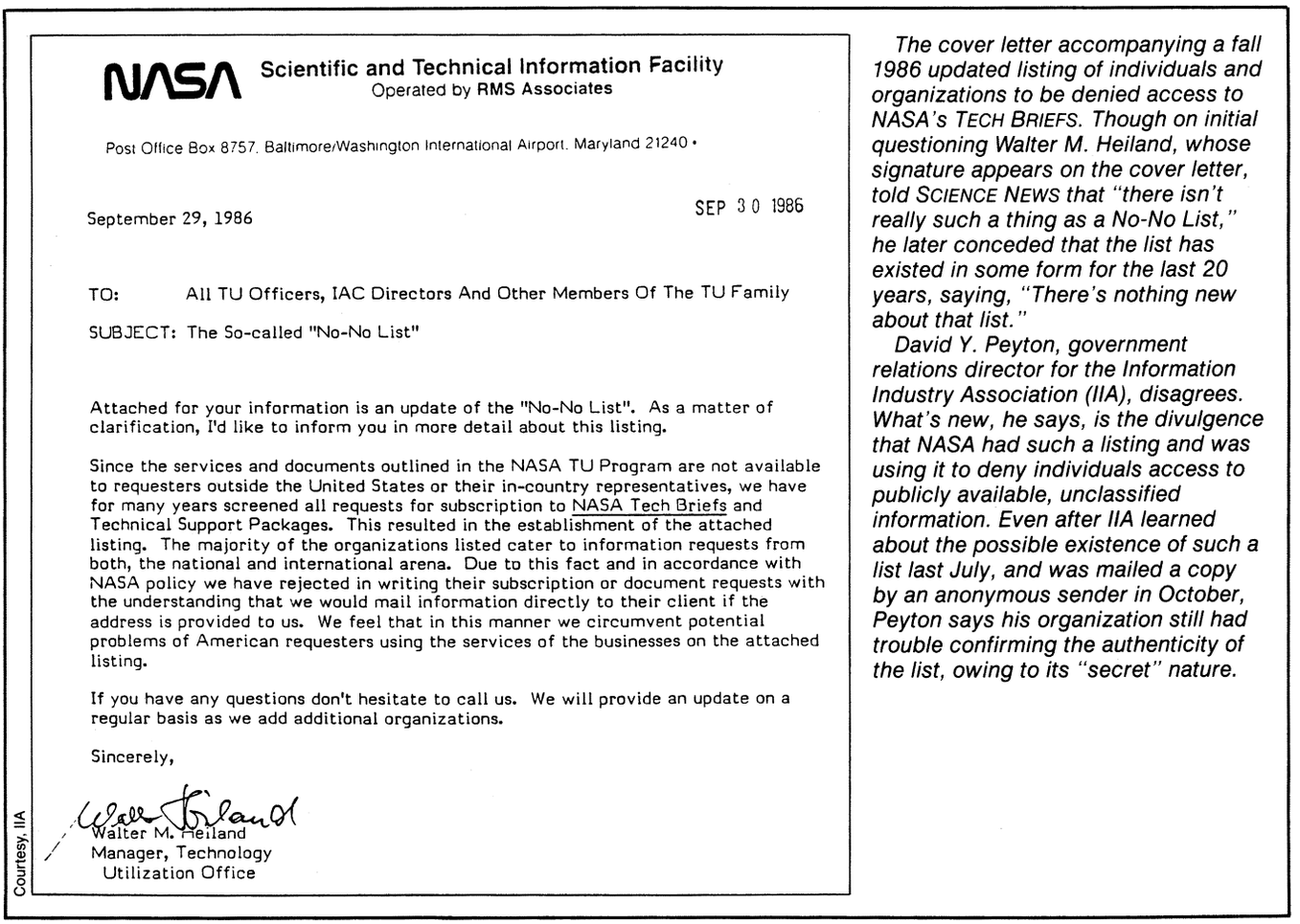
The discussions involved how best these agencies might implement new measures consistent with National Security Decision Directive-145, or the National Policy on Telecommunications and Automated Information Systems Security. Portions of the 10-page directive, issued in September 1984, deal with how to safeguard nonclassified data in private data bases. For example, it says, when doing so would benefit national security, "the private sector shall be encouraged and advised, and where appropriate assisted," by the federal government in adopting new data-security measures.

What kinds of data were envisioned as falling under this directive? Potentially the kind Simpson's company now sells — the texts of unclassified government reports, newspaper articles, wire-service stories or other documents typical of what might be found at a public library.

The directive says that "such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate." To protect this, NSDD-145 proposed a new category of controllable data: "sensitive but unclassified government or government-derived information, the loss of which could adversely affect the national security interest." According to the White House directive, this information "shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security."

The commercial information industry had few clues on whether or how the federal government intended to implement NSDD-145 until high-level national security officials began making the rounds and talking to owners of some of the nation's biggest commercial data bases last year.

Simpson says those officials asked whether he might consider restricting the sale of any sensitive but unclassified data he might have to Eastern Bloc customers. They asked whether, alternatively, he would consider instituting on-line monitoring of various customers' requests so that subscribers interested in potentially sensitive subjects might be surreptitiously identified.



NASA Scientific and Technical Information Facility
Operated by RMS Associates

Post Office Box 8757, Baltimore/Washington International Airport, Maryland 21240 •

September 29, 1986 SEP 30 1986

TO: All TU Officers, IAC Directors And Other Members Of The TU Family

SUBJECT: The So-called "No-No List"

Attached for your information is an update of the "No-No List". As a matter of clarification, I'd like to inform you in more detail about this listing.

Since the services and documents outlined in the NASA TU Program are not available to requesters outside the United States or their in-country representatives, we have for many years screened all requests for subscription to NASA Tech Briefs and Technical Support Packages. This resulted in the establishment of the attached listing. The majority of the organizations listed cater to information requests from both, the national and international arena. Due to this fact and in accordance with NASA policy we have rejected in writing their subscription or document requests with the understanding that we would mail information directly to their client if the address is provided to us. We feel that in this manner we circumvent potential problems of American requesters using the services of the businesses on the attached listing.

If you have any questions don't hesitate to call us. We will provide an update on a regular basis as we add additional organizations.

Sincerely,

Walter M. Heiland
Manager, Technology
Utilization Office

Courtesy, IIA

The cover letter accompanying a fall 1986 updated listing of individuals and organizations to be denied access to NASA's TECH BRIEFS. Though on initial questioning Walter M. Heiland, whose signature appears on the cover letter, told SCIENCE NEWS that "there isn't really such a thing as a No-No List," he later conceded that the list has existed in some form for the last 20 years, saying, "There's nothing new about that list."

David Y. Peyton, government relations director for the Information Industry Association (IIA), disagrees. What's new, he says, is the divulgence that NASA had such a listing and was using it to deny individuals access to publicly available, unclassified information. Even after IIA learned about the possible existence of such a list last July, and was mailed a copy by an anonymous sender in October, Peyton says his organization still had trouble confirming the authenticity of the list, owing to its "secret" nature.

Their concern, Simpson recalls, was that while a newspaper article might contain only a piece of a puzzle, if that article is sold along with the texts of related items, such as government reports, speeches or congressional hearings transcripts, the sum might turn out to be more dangerous — and therefore more in need of controls — than the individual pieces.

This decades-old concept is known as the "mosaic or compilation theory," explains Steve Garfinkel of the General Services Administration's Information Security Oversight Office. His department seeks to prevent abuse of the federal classification system. In the past, Garfinkel says, mosaic theory has been used to justify only the *classification* of data — not restrictions on the publication of *unclassified* material.

But an Oct. 29, 1986, policy statement on data-base security by John Poindexter, the recently resigned White House national security adviser, suggests that evolving administration policy indeed intended to extend mosaic theory. Specifically, it says that the "disclosure" of "sensitive, but unclassified information ... could adversely affect national security or other federal government interests." To protect those interests, the statement requires the director of the CIA to identify such information and to establish "the protection required for such information." It also calls for the development, funding and applications of new security measures or systems "as appropriate, to satisfy [these] security or protection requirements."

Garfinkel says that if mosaic theory were used to justify controls on material the government concedes is unclassified, it would constitute a major broadening of this concept's administration, and one he says he has always assumed would be legally unenforceable.

But not necessarily unthinkable. He notes that in the past few years several government agencies "have taken [this theory] a little bit farther than it's ever been taken before." And in at least one or two of those cases, he told SCIENCE NEWS, "they've taken it too far," necessitating behind-the-scenes moves by his office to redress the situation.

The American Civil Liberties Union (ACLU) believes the administration also anticipated that its expansion of mosaic theory would be legally unenforceable, and therefore resorted to merely "suggesting" that commercial data vendors like Mead Data Central voluntarily control their data. Voluntary enactment of such measures, says Jerry Berman, chief legislative counsel in the ACLU's Washington, D.C., office, would get around the need to test their legality.

But Simpson had no intention of offering Mead Data Central's voluntary compliance. Nor did the Information Industry Association (IIA), a Washington, D.C.-based association of 460 private companies that specialize in disseminating computer data. In a Dec. 17, 1986, letter to Defense Secretary Caspar Weinberger, IIA President Paul G. Zurkowski charged that "certain persons within the U.S. defense establishment—in a manner that is inconsistent with democratic principles and law—are attempting to restrict or monitor citizen access to unclassified information now available to the public. Such restrictions on the flow of unclassified information could severely limit the information available to citizens, have a chilling effect on those who wish to acquire information, restrict our nation's technological development, and hinder the ability of U.S. companies

to do business."

A Jan. 9 response by Donald C. Latham, chairman of the Defense Department's National Telecommunications and Information Systems Security Committee, said "the scope, purpose and applicability of the policy is being misunderstood." But the letter did not assuage IIA's concerns nor the ACLU's.

IIA pointed out, for example, that Latham's letter not only contradicted previous statements he had made before Congress on the intended scope of new NSDD-145-based controls, but also ignored IIA's concern about controversial recommendations contained in a new, classified Air Force study. Simpson says the national security officials who visited data-base vendors last year mentioned that their suggestions for new controls had been spurred at least in part by recommendations in this study.

David Y. Peyton, director of government relations for IIA in Washington, D.C., says he's "been told by people who have read the Air Force study" that it makes 27 recommendations for protecting sensitive information stored in electronic-data-retrieval systems – including commercial ones. Among the most troubling, according to IIA, is a recommendation that commercial data vendors restrict their foreign sales of unclassified data to licensed customers. Currently, they can sell these data freely to all.

On March 17, apparently responding to pressure from the IIA and others, Frank C. Carlucci III, newly appointed as the administration's national security adviser, delivered a letter to Rep. Jack Brooks' (D-Tex.) House subcommittee on legislation and national security. It said that the administration was not only withdrawing Poindexter's Oct. 29 policy statement, but also reconsidering the need for NSDD-145 and its new category of "sensitive but unclassified information."

While IIA and the ACLU's Berman view this as a triumph of the concerted public campaigning they launched over the issue, neither is satisfied with the gesture. Peyton of IIA says the problem of what restrictions might be imposed on commercial, nonclassified data "isn't solved by any means." He notes that a nonclassified summary of the Air Force report still isn't available, FBI counterintelligence agents are still making intimidating visits to IIA member companies, and NSDD-145 and "its shadowy definition of sensitive information remains in effect."

Finally, there is the case of Michael Radnor, director of Northwestern University's Center for the Interdisciplinary Study of Science and Technology (CISST), in Evanston, Ill. Late last year he learned that NASA had included his name on its little-known "No-No List," an informal compilation of individuals and companies that would not be allowed to subscribe to NASA TECH BRIEFS. The 10-times-yearly magazine, available free to some 150,000 U.S. scientists, engineers and businesses, offers nonclassified descriptions of new technologies resulting from NASA research.

The existence of the list was revealed late last year by IIA in an announcement to its members and to the public. IIA provided SCIENCE NEWS with the list and an accompanying cover letter, signed by Walter M. Heiland, manager of NASA's Technology Utilization Office, describing the listed parties as having ties with foreign countries, firms or agencies. Radnor's offense, according to the list, was that CISST ran a technology-transfer program with Japan. Funded by the State of Illinois, this program seeks out foreign technologies of possible use to Illinois businesses.

Radnor notes that while Heiland initially denied to him the existence of a "No-No List," he later promised to take Radnor's name off of it once he learned CISST was sharing Japanese data, not U.S. technologies. When Heiland was questioned by SCIENCE NEWS about the list, he responded, "There isn't really such a thing." But he then acknowledged that a list does exist, that Radnor's name "got on the list through a misunderstanding" and that the list "reflects NASA policy . . . that documents and services available through the [NASA] Technology Utilization Program are not available to requesters outside of the United States or their in-country representatives." Heiland added that such lists have existed for 20 years, but that their distribution has always been "internal."

This has not placated Radnor. He says he considers the listing carelessly prepared (since its compilers never checked with Radnor's group to discern which country's technology was getting transferred), "extralegal" (because it attempts to place controls on unclassified, nonsensitive data) and "immoral" (by impugning Radnor's character – as a potential foreign agent – to any recipients of the list). Even if the listing were legal, Radnor says, it's "stupid," since anyone prevented from subscribing to NASA TECH BRIEFS can get the magazine at their local library.

After initially asking Heiland to send a retraction to all original recipients of the list, and getting no response, Radnor is now having the university's lawyers petition their senators to investigate this matter.

Berman, who directs the ACLU's Project on Information Technology and Civil Liberties, says the three programs described here are not isolated instances, but part of a "broad," stepped-up "attack by the Reagan administration to control scientific and technical information in the name of national security."

He is also concerned, he says, about the recent participation of CIA and National Security Agency officials in visits to data-base vendors. Their "suggestions" about voluntary monitoring of who gets access to unclassified data indicate an interest in domestic intelligence surveillance – perhaps, he says, with an eye toward extending that surveillance beyond what is now permitted by law.

"These are very troubling times," says Mead Data's Simpson. It's the classic battle of national security vs. freedom of speech, he says, and security is winning. Berman agrees, adding that "in the face of government pressure and in the current legal environment, the scientific community has read the writing on the wall and has moved increasingly toward self-censorship."

Simpson would look to the Congress for relief. Berman would look to a political consortium of the affected parties. But Stephen Gould, project director of the American Association for the Advancement of Science's program on scientific communications and national security, would throw the responsibility for motivating change back in the lap of the research community. "It is the unwanted responsibility of the research community to document the costs of regulation," says Gould, "and seek relief if serious disruptions in the advancement of science and technology can be proven." □