OSI: Better the Devil You Know?

Reaction to proposed changes in misconduct investigations suggests just how difficult it could be to fix a system that has been widely criticized

NIH's OFFICE OF SCIENTIFIC INTEGRITY (OSI), born 3 years ago largely because of congressional complaints that the universities had proved themselves incapable of investigating allegations of scientific misconduct, now seems about to become a victim of similar complaints. For most of the past year, the office has taken a beating at the hands of nearly everyone who has come in contact with it, whether scientists under investigation and their lawyers, other researchers who want to see it police their profession more efficiently, university administrators, legislators, or the NIH director herself. The office staff is incompetent, some say. The process denies constitutional guarantees and basic fairness to those it investigates, say others. The complaints go on: The office has succumbed to unwarranted political influence. It's too slow. It confuses investigations with adjudications. Now NIH's parent agency, the Public Health Service (PHS), has proposed yet another cure-all (*Science*, 6 March, p. 1199)—in effect declaring that OSI's "scientific dialogue," an attempt to settle misconduct allegations through a scientific approach instead of a legal one, has been a failure. Its proposal has gone to Health and Human Services (HHS) Secretary Louis Sullivan.

But as scientists get a better look at the bureaucracy suggested as a replacement for OSI, they could find they risk trading a devil they know for one they don't. For instance, in an attempt to reduce potential conflicts of interest where investigations of NIH researchers and grantees are concerned, the plan would shift OSI out of NIH into the office of Assistant Secretary of Health James Mason—the health official responsible for enforcing the Bush Administration's ban on research using human fetal tissue. And, by giving scientists accused of misconduct the right to request adjudicatory hearings, the proposal could result in PHS officials having power to subpoena witnesses in misconduct hearings, and might routinely make the details of allegations public. In fact, the reorganization plan provoked such a storm of discussion at a meeting last weekend of a PHS advisory committee, chaired by University of Michigan historian Nicholas Steneck, that its reception in the scientific community seems likely to be bumpy.

On its face, the reorganization plan appears straightforward. In addition to renaming OSI the Office of Research Integrity Assurance (ORIA) and assigning it to Mason's office, the proposal would essentially do away with the Office of Scientific Integrity Review (OSIR), which currently reviews the results of OSI's investigations before passing them on to Mason. OSIR would become an executive staff for the Research Integrity Policy Board—a new committee of PHS officials chaired by the NIH director that would advise Mason on PHS misconduct policy—and its reviewing responsibilities would be taken over by a new adjudicatory panel in Sullivan's office. Any scientist accused of misconduct by ORIA could request a hearing before this panel, which would consist of a hearing officer drawn from the departmental contract appeals board and two scientific advisers.

The proposal to add a round of hearings to the process is probably the most significant change being considered. Members of the Steneck committee hailed the proposal, which they had informally recommended last November as a way of answering complaints that OSI does not protect the constitutional "due process" rights of those it investigates. Under existing PHS rules, scientists can request public hearings only when threatened with debarment from federal funding—the strongest sanction the government can impose. Federal officials defend this process as consistent with the precedents of administrative law. But critics such as Barbara Mishkin, a Washington lawyer who has defended scientists under OSI investigation, argue that the label of misconduct itself imposes such a heavy penalty that more due process is necessary. "They think if they haven't debarred someone, it's not a serious action," she says. "It's not the sanction but the label that damages someone's reputation."

In practice, however, hearings could have several unexpected consequences. For instance, PHS has not yet decided whether to open such hearings, but if it follows the model of debarment hearings, these proceedings will be public—a fact that might make researchers accused of misconduct think twice before requesting one. "The issue of confidentiality is terribly important to the accused, given the danger that their reputations can be irreparably damaged," says Estelle Fishbein, a member of the PHS panel and general counsel for Johns Hopkins University. But secret trials, she said, could be just as dangerous for different reasons. "When something is at the level of a federal administrative agency, I guess maybe the accused would feel best protected by an open hearing."

Routine misconduct hearings could also end up incorporating many of the formal elements of criminal and civil trials—includ-

"Scientific dialogue" vs. legal approach. *OSI director Jules Hallum, attorney Barbara Mishkin, and Johns Hopkins University counsel Estelle Fishbein.*

What's Left on the Table

If Secretary of Health and Human Services Louis Sullivan accepts the proposal to shift the Office of Scientific Integrity (OSI) out of NIH and provide hearings for those deemed to have committed scientific misconduct, some of the complaints raised by OSI's critics would be met (see main text). But many other divisive issues have not been addressed by the plan—issues such as the kinds of alleged misdeeds that should trigger an investigation, how the investigations should be conducted, and who should carry them out.

Definitions. Within the research community, most objections to the current system have begun with the government's use of the term "scientific misconduct," defined in Public Health Service (PHS) regulations as falsification, fabrication, plagiarism, or other practices that "deviate seriously" from those commonly accepted. (The National Science Foundation [NSF] uses a similar definition that includes retaliation against good-faith whistleblowers as an additional clause. The PHS definition explicitly exempts "honest error," while NSF does not.) Federal officials like this definition because it sidesteps the requirement to prove intent—which is built into the usual legal meaning of fraud—and it allows the government to take action in unusual circumstances, such as allegations of professional blacklisting and abuse of the peer-review system.

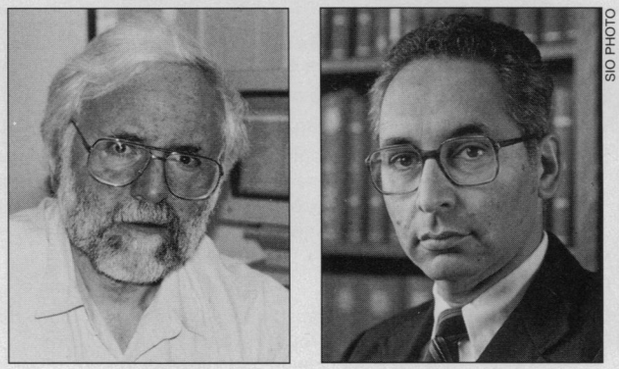
But some scientists and lawyers complain that the definition is far too broad, allowing the government to interfere in cases where it has no business. Just last weekend, a PHS advisory panel unanimously recommended junking the term "scientific misconduct" in favor of "research fraud," which it defined as plagiarism, fabrication, and intentional falsification, or other "deliberate misrepresentation" of research. The intention, says Paul Friedman, a panel member and dean of academic affairs at the University of California, San Diego, is to draw a clear line "between really serious, lawbreaking misconduct and the sort of stuff that you'd like to deal with, but not through the agencies of the federal government."

But federal misconduct officials argue that limiting the definition could leave real instances of wrongdoing unaddressed at the federal level. "On a case by case basis, we're learning what's out there," says James Zwolenik, NSF's assistant inspector general for oversight. "It would be rash for the government to drop the 'other practices' clause." OSI director Jules Hallum, meanwhile, says complaints with the definition stem from "a perception of how the [existing] definition is used, not the reality." Instead of revising the definition, Hallum suggests, researchers should let his office establish some "common law" precedents in applying it. Even some scientists agree: Harvard biochemist Paul Doty says he supports the existing definition, noting that "you have to have a definition that covers situations that you can't even now conceive of."

Government vs. universities. Friedman would prefer to leave the investigation of less serious misconduct allegations to universities. But OSI was set up partly in response to several cases in which universities failed to investigate allegations thoroughly, and it now requires universities to submit their final investigative reports for federal review. Universities, however, are not required to report fact-finding inquiries that find no misconduct, a loophole that could allow them to "quash everything at the inquiry stage," says Arthur Raines, a pharmacologist at Georgetown.

Raines suggests that OSI review all inquiry reports. But Estelle Fishbein, a lawyer at Johns Hopkins University, rejects that idea, noting that inquiries were specifically designed to avoid tainting the reputations of people who have done nothing wrong. Instead, she suggests, OSI could require universities to inform whisteblowers of their right to take allegations to a higher authority.

In cases where universities still do not handle allegations well, OSI can do little but point out their deficiencies and investigate the cases itself. While OSI can theoretically yank all of an institution's federal funding, Hallum describes that power as "using an atom bomb to swat a butterfly." Drummond Rennie, a member of the PHS panel and West Coast editor of the *Journal of the American Medical Association*, argues that "there have to be federal oversight and sanctions—not just against individuals, but against universities that don't handle things properly." Tina Gonzalez, associate vice chancellor for research at the University of Illinois, agrees that "issues of accountability are real." But she adds that the government should take action only after a university has completed an investigation, "and then hold their feet to the fire if necessary."



SIO PHOTO

Is science a special case? *Drummond Rennie* (left) *says no, Paul Friedman says yes.*

The big picture. Pervading much of the debate over how to handle scientific misconduct is a topic that is rarely discussed openly: Should suspected wrongdoing in science be treated any differently from misconduct in other professions such as law or finance, whose practitioners are subject to extensive government regulation aimed at keeping them honest?

Friedman believes so, suggesting that overzealous regulation of misconduct may be so disruptive to science that the benefits to society will outweigh the costs. "In terms of the social good it provides, perhaps science does need to be treated differently," he says. "I'm sorry if that sounds like special pleading." Rennie, on the other hand, suggests that scientific misconduct will one day be subsumed entirely into administrative law. "Everybody's got to grow up," he says.

Echoing Rennie is a staff aide to Representative John Dingell (D–MI): "There are two ways of dealing with misconduct—either you don't expose it and go back to the good old days, or you get into prevention.... I haven't seen any [community] effort put into prevention, which tells me they want to go back to the good old days." Three years after the experiment to have NIH investigate itself and its grantees was begun, this chasm is as broad as ever. ■ **D.P.H.**

NSF's No-Fuss Investigations

Although the National Institutes of Health manages only a fraction of the federal government's R&D budget—$9 billion out of $75 billion, or about 12%—it has had a virtual monopoly on prominent cases of scientific misconduct. Yet the National Science Foundation's (NSF) inspector general investigates almost as many misconduct allegations as NIH's Office of Scienctific Integrity (OSI) each year, with relatively little public fuss. Does NSF know something about conducting investigations that has escaped OSI?

Some critics of NIH's misconduct investigations think so. Assistant inspector general for oversight James Zwolenik, a Ph.D. physical chemist who now oversees most NSF misconduct cases, credits his office's apparent success to an unusual synthesis of scientific, legal, and investigative expertise on which it relies to resolve cases of alleged misconduct. Lawyers are involved at every stage of typical NSF misconduct investigations, from routine correspondence to the preparation of draft reports. The office can also call on two trained investigators (who normally spend their time unraveling financial wrongdoing in NSF grants and contracts) to unearth documents and interview witnesses. Zwolenik and two staff scientists oversee operations and draft the investigative reports, which they then turn over to the NSF deputy director for adjudication. OSI, in contrast, has only recently obtained a full-time lawyer who now plays a prominent role in that office's investigations.

HOW NSF STACKS UP AGAINST OSI

	Office of Scientific Integrity	National Science Foundation
Location of Office	Office of the NIH director	Office of Inspector General
When Created	16 March 1989	10 February 1989
Staffing	2 scientist-administrators 6 "caseworkers" 8 support staff One lawyer on call	3 scientist-administrators 2-member legal staff 2 trained investigator/auditors
Number of Allegations Received in 1991	70	52
Cases Typically Encountered	Plagiarism, abuse of the peer review system, data fabrication and falsification	Plagiarism and "intellectual theft"

Because the NSF operation is run by the inspector general, who is responsible only to Congress and not to the NSF director, it has been insulated from charges of political interference. OSI, on the other hand, currently reports to the NIH director, and under a proposed reorganization (see main text) would report to another political appointee, the assistant secretary for health. NSF also cannot take any action against a scientist's funding until the deputy director has made a finding of misconduct, whereas NIH notifies its institute directors through the ALERT system when researchers under investigation come up for new grants or positions, and at least once has blocked a grant renewal because of evidence turned up in an ongoing investigation.

In a legal sense, the most significant difference between the two models may be the fact that NSF consults scientists individually as expert witnesses, whereas OSI convenes expert panels to offer their views on whether misconduct has taken place in cases involving allegedly "deviant" scientific practices. Panel members can also publicly dissent from the conclusions in final reports, suggesting that OSI allows them to vote on misconduct findings. In private, NSF attorneys are scathingly critical of this arrangement, arguing that OSI's panels appear to pass judgment on cases at the investigative stage. "What [the panels] find is likely to be locked in stone," says one. OSI director Jules Hallum denies that any adjudication is involved at the investigative stage.

There's one aspect of NSF's system that may color perceptions of its operations: It has never had to deal with complex and divisive cases like OSI's investigations of NIH AIDS researcher Robert Gallo and a paper co-authored by Nobel laureate David Baltimore, both of which have given that office much public grief. In fact, NSF has rarely had to investigate any allegations of data falsification or fabrication; its caseload consists mostly of charges of plagiarism and intellectual theft. As a result, NSF has not faced the trial by fire to which OSI has been subjected in the past 3 years. ■ **D.P.H.**

ing additional government authority such as subpoena power. "I personally would like subpoena power to the extent it's required by the hearing process," PHS attorney Chris Pascal told the advisory committee. Without it, he said, his agency could not compel individuals involved in a case to testify as witnesses for either side—a situation that could certainly hurt an accused scientist who wanted to cross-examine a reluctant whistleblower. OSI director Jules Hallum objected vehemently, arguing that such a move would further erode scientists' control over the processes of science. "If you want to generate controversy, this is how you'd do it" he said. "You will have set up OSI as the police agency of science."

Furthermore, Pascal suggested, if the federal government gives accused scientists an opportunity to have a public hearing on misconduct charges, it might want to require universities to do the same. Noting that OSI now bases most of its misconduct findings on the results of university reports, rather than its own investigation, he said that basic fairness and the committee's desire to let universities control as much of the misconduct process as possible argued for university hearings. But the prospect of further government mandates for universities did not appear to sit well with committee members. "I'd like to see less involvement with government," said Fishbein. "I think that should be left to each university." Instead, most members preferred to encourage universities to offer such hearings voluntarily.

Finally, by offering investigative subjects additional due process, a formal hearing could conceivably strip OSI's investigations of existing due process protections. Currently, the office allows the subjects of its investigations to rebut a draft report at the end of an OSI investigation. It also provides accused scientists copies of any evidence it is citing against them, Hallum told the committee. The office then revises its report—often substantially, Hallum says—and appends any rebuttals before sending the entire package to OSIR for review. With hearings in place, however, Hallum said he could imagine that one day OSI might no longer allow such rebuttals except in an adversarial hearing. (Hallum added that he would "strive mightily" to retain the existing system.)

Hallum also told the committee that losing the case review now provided by OSIR would mean that cases in which OSI finds no misconduct would not get a second look. (Such cases are never revealed to the public—a policy currently under court challenge in a Freedom of Information Act lawsuit brought by NIH researcher Charles

McCutchen.) "If there's no misconduct, there's no one checking to say we didn't do a sufficient investigation," Hallum said. "We could be in the whitewashing business for all anyone would know." While committee members discussed the possibility of having Mason's office conduct this sort of review, they made no final recommendation.

For now, reforms for OSI are still some time away. Sullivan has apparently given no sense of when he might deal with the reorganization proposal, and if he does approve policy changes they must still be published in the *Federal Register* for public comment before they are enacted—a process that can take months. In the meantime, reformers will have to deal with yet another power center: Congress. The House version of the NIH reauthorization bill enshrines the current definition of misconduct and would keep OSI right where it is, a fact that alarmed several committee members. But an aide to health subcommittee chairman Representative Henry Waxman (D–CA) says that provision was drawn up last year before PHS began to revise its procedures, and that both the House and the Senate are likely to be sympathetic to the agency's reforms. But the aide suggests that Congress could act quickly once Sullivan makes up his mind, meaning that scientists may end up living with whatever changes emerge from this process for a long time. ■ **DAVID P. HAMILTON**

Fatal Error: How Patriot Overlooked a Scud

Even a minute mathematical error can lead to tragedy in the computer age, as confirmed by a report on the Patriot missile issued by the General Accounting Office (GAO) last week. The report describes how a minor bug in Patriot's software allowed an Iraqi Scud missile to slip through Patriot defenses a year ago and hit U.S. Army barracks in Dhahran, Saudi Arabia, killing 28 servicemen.

GAO undertook the study on orders from Representative Howard Wolpe (D–MI), who says he has questions about whether the military's "logistical apparatus is adequate to support...software-driven weapons." He was not reassured. "The episode," Wolpe wrote in a letter to Defense Secretary Richard Cheney, "makes clear the problems American troops may face as we continue to take advantage of the benefits of the computer revolution in developing weapons."

According to the GAO report, the Patriot's electronic brain—now 20 years old—would have performed well in the task it was designed to do, which was to track and shoot down relatively slow-moving aircraft. But it ran into trouble when it was pressed into service in the Persian Gulf to defend against high-speed ballistic missiles. The main flaw was in the way the Patriot battery's missile-tracking computers processed timing information, which affected its ability to pinpoint the location of fast-moving targets.

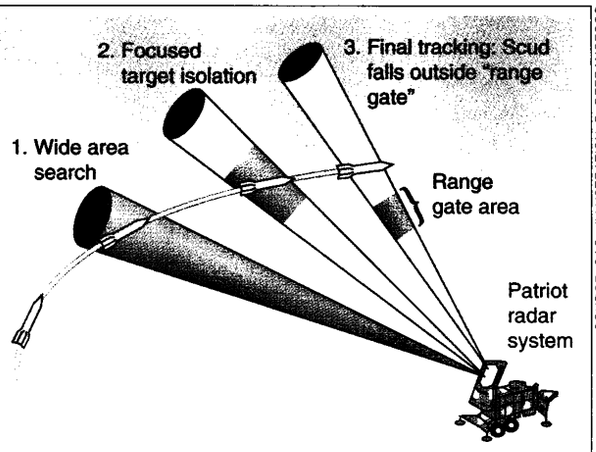
The computer's tracking calculations depended on signals from its internal clock, which it translated into a "floating point" mathematical value. Because the computer could handle only relatively small chunks of data (by today's standards), it was forced to truncate this time value slightly, creating a slight error. By itself, the flaw would not have been fatal, but the Patriot software was written in a way that caused the error to increase steadily as time passed on the computer's clock.

That's what happened on the night of 25 February 1991. A Scud missile launched from Iraq popped over the horizon in Saudi Arabia and was picked up by a Patriot's radar, which was then performing a wide search of the sky. The Patriot locked onto this target and calculated a "track" that was an approximation of the path it would follow to the ground. To confirm that this was truly an enemy Scud, the computer was programmed to get a second radar sighting to determine whether the object was following the path expected of a ballistic missile. If it was not, the signal would be rejected as a false alarm. And to speed up the process, the software told the computer to analyze only data from a small portion of the radar beam—the portion within a mathematically limited zone (the "range gate") centered on the path that a ballistic missile would be expected to follow. If the computer found a target within this range gate, it would know that the attack was real and would launch a Patriot missile. Sadly, in this case the computer miscalculated the position of the range gate, failed to see the Scud, and ruled that the original signal was a false alarm.

The mistake occurred because this particular Patriot battery had been running continuously for about 100 hours. According to GAO, its logic had built up a timing lag of 0.3433 second. That may sound trivial, but when tracking targets traveling at ballistic speeds the error was fatal, for it caused the computer to shift the range gate 687 meters, letting the Scud pass unnoticed.

Ironically, about a week before the Dhahran tragedy, U.S. military officials had been warned that something like this could happen, according to GAO. The warning came first from the Israeli military, which had been analyzing data records from Patriot batteries in Israel. The Israelis discovered that after about 8 hours of continuous use, the Patriot system built up a timing error of 0.0275 second, enough to create a range-finding error of about 55 meters. They passed the word to the U.S. Patriot project office on 11 February 1991.

Within a few days, the Patriot project office made a software fix correcting the timing error, and sent it out to the troops on 16 February 1991. On 21 February, the office sent out a warning that "very long run times" could affect the targeting accuracy and alerted officers to the fact that new software was on the way. The troops were not told, however, how many hours "very long" was, or that it would help to switch the computer off and on again after 8 hours. The U.S. forces finally solved the timing problem when they received and installed the new software at Dhahran on 26 February—a day too late. ■ **ELIOT MARSHALL**



SOURCE: GAO ILLUSTRATION: D. DEFRANCESCO

Fatal software bug. *A timing flaw in the Patriot's software caused its computer to focus the target analysis ("range gate") on the wrong segment of the radar beam, failing to detect an incoming Scud.*