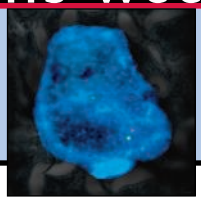
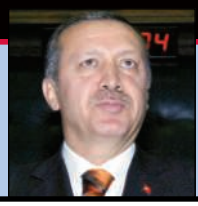
This Week



PAGE 603
A cause of prostate cancer?



605
Cronyism in Turkish science

SCIENTIFIC COMMUNITY

'Security Breach' Leaks NIH Grant Applications Onto Web

When Leemor Joshua-Tor received an e-mail from the National Institutes of Health (NIH) earlier this month regarding her recent grant application, the structural biologist at Cold Spring Harbor Laboratory in New York was hoping for good news. After all, a study section had ranked the proposal highly in June. Instead, the agency informed her that her application—containing a large amount of unpublished data relating to a project she had been working on for 10 years—had been posted on the Internet, freely accessible to the public.

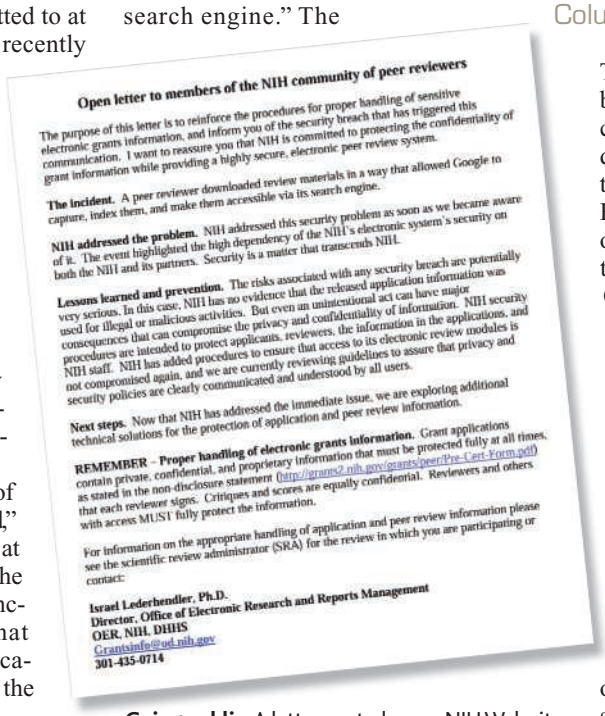
Joshua-Tor was not alone. One hundred and forty grant applications submitted to at least one NIH study section were recently released onto nonsecure Web pages. NIH has been mum about the leaks, citing only a "security breach" and vaguely alluding in a Web-posted open letter to the actions of a peer reviewer. More surprising, the agency has not informed all individuals affiliated with the study section about the incident and has not shared basic information with affected authors regarding exactly when or for how long their supposedly secure proposals were available for public consumption.

"This is the first time I've heard of this happening, and it chills my blood," says Julio Fernandez, a biophysicist at Columbia University, who chairs the Macromolecular Structure and Function C (MSFC) study section that reviewed Joshua-Tor's grant application. "It's an unthinkable attack on the entire system."

NIH spokesperson Don Ralbovsky says the agency can't discuss the specifics of the leak for security reasons. NIH would also not comment on why all affected authors had not been contacted or why individuals affiliated with the MSFC study section, including Fernandez and a number of peer reviewers who served on the section in June and February, had not heard of the incident before *Science* brought it to their attention.

Confused and frustrated by the initial NIH e-mail, Joshua-Tor requested more information. She found the agency's response unsatisfying. Israel Lederhendler, the director of NIH's Office of Electronic Research and Reports Management, directed her to an open letter posted on the agency's grant Web site.* It stated that "a peer reviewer downloaded review materials in a way that allowed Google to capture, index them, and make them accessible via its search engine." The letter added that NIH had addressed the problem and was taking steps to ensure that it didn't happen again. But Joshua-Tor is still left with unanswered questions: "The letter didn't say what exactly had gone up [on the Web] or how long it had been up," she says.

> "It chills my blood. … It's an unthinkable attack on the entire system."
>
> —Julio Fernandez, Columbia University



Open letter to members of the NIH community of peer reviewers

The purpose of this letter is to reinforce the procedures for proper handling of sensitive electronic grants information, and inform you of the security breach that has triggered this communication. I want to reassure you that NIH is committed to protecting the confidentiality of grant information while providing a highly secure, electronic peer review system.

The incident. A peer reviewer downloaded review materials in a way that allowed Google to capture, index them, and make them accessible via its search engine.

NIH addressed the problem. NIH addressed this security problem as soon as we became aware of it. The event highlighted the high dependency of the NIH's electronic system's security on both the NIH and its partners. Security is a matter that transcends NIH.

Lessons learned and prevention. The risks associated with any security breach are potentially very serious. In this case, NIH has no evidence that the released application information was used for illegal or malicious activities. But even an unintentional act can have major consequences that can compromise the privacy and confidentiality of information. NIH security procedures are intended to protect applicants, reviewers, the information in the applications, and NIH staff. NIH has added procedures to ensure that access to its electronic review modules is not compromised again, and we are currently reviewing guidelines to assure that privacy and security policies are clearly communicated and understood by all users.

Next steps. Now that NIH has addressed the immediate issue, we are exploring additional technical solutions for the protection of application and peer review information.

REMEMBER – Proper handling of electronic grants information. Grant applications contain private, confidential, and proprietary information that must be protected fully at all times, as stated in the non-disclosure statement (http://grants2.nih.gov/grants/peer/Pre-Cert-Form.pdf) that each reviewer signs. Critiques and scores are equally confidential. Reviewers and others with access MUST fully protect the information.

For information on the appropriate handling of application and peer review information please see the scientific review administrator (SRA) for the review in which you are participating or contact:

Israel Lederhendler, Ph.D.
Director, Office of Electronic Research and Reports Management
OER, NIH, DHHS
Grantsinfo@od.nih.gov
301-435-0714

Going public. A letter posted on an NIH Web site blames the grant leak on a peer reviewer.

Some affected scientists have yet to hear from NIH. Stephen Sprang, a biochemist at the University of Texas Southwestern Medical Center in Dallas, found out about his grant application going public from a colleague, who discovered Sprang's proposal to the February MSFC study section as well as his own on the Web. "My reaction at the time was, 'This is odd and inappropriate,' " Sprang says. "Grant applications are presumably private, and this felt like an invasion of privacy." Still, he says, it's difficult to assess the consequences of the leak without knowing further details.

One scientist whose grant proposal to the June MSFC study section was also made public believes NIH's eRA Commons site, designed for the electronic exchange of grant information, may have been the source of the leak. The scientist, who declined to be named because his application is still pending, came across his proposal on the Web while doing a Google search for more information on software he uses in his research. He says he was able to access a number of other applications simply by entering the terms "sketch site: era.nih.gov" into Google. When *Science* performed the search, it brought up several grant titles, but the proposals themselves were no longer available.

Some worry that such security lapses could compromise NIH's ambitious plans to make its grant application and review process entirely Web-based. The agency plans to have all grant proposals submitted electronically by May 2007. "I'm sure there will be additional problems," says Vernon Anderson, a biochemist at Case Western Reserve University in Cleveland, Ohio, and a peer reviewer on another MSF study section. Still, he says, "personally, I'm more worried about someone getting my Social Security or credit card number than my grant information." And he notes that even before electronic submissions, there was always the concern that peer reviewers would steal ideas from an applicant's proposal. "But at least then, if someone stole your idea, you could trace it back to the study section," he says. "Now, if something goes up on the Web, there's no way to trace who saw it."

–DAVID GRIMM

CREDIT: NIH

*grants1.nih.gov/grants/letter_to_peer_reviewers.pdf

Published by AAAS