DOD'S NEW ANTI-LEAK PLAN: TURN MICHAEL VICKERS INTO A BLOGGER

DOD just rolled out its new plan to combat national security leaks. (h/t Jason Leopold) At its core is a "top-down" approach: to have the Under Secretary for Defense of Intelligence, Mike Vickers, to review all major reporting to look for leaks.

> To ensure greater accountability and tracking of unauthorized disclosures, Secretary Panetta is directing a new "top down" approach as well. The Undersecretary of Defense for Intelligence, in consultation with the Assistant Secretary for Public Affairs, will monitor all major, national level media reporting for unauthorized disclosures of defense department classified information.

One one level this seems like a good idea. I mean, I'm a blogger, and I usually have a better idea of who's leaking than the people overseeing Executive Branch agencies. But hey, I don't want to shortchange journalists; Walter Pincus performs a nice bit of leak debunkery with this piece, for example.

But there does seem to be one problem with the plan to have Mike Vickers watch for any security breaches. Doesn't he have a day job? Isn't he supposed to be watching the Taliban and China and cyberattacks? Have we gotten so paranoid that one of our top intelligence people is going to spend his time watching journalists than watching our military enemies?

On another issue, though, DOD is to be congratulated. Today's release also revealed that, within the last few months, it has put in

place the no-brainer security fixes that it promised in response to the WikiLeaks breach.

> Lockdown of removable storage device use on the Defense Secure Network (SIPRNET). The department has deployed a host-based security system (HBSS) tool to virtually monitor every defense department computer. HBSS prevents the downloading of information onto removable storage like DVDs, CDs, and memory sticks, with very limited exceptions. The tool also sends an alarm any time someone tries to write classified information to such removable storage. For authorized exceptions, the tool audits any downloads of information.
>
> Improved monitoring of DoD networks. The department issued a cyber identity credential (Public Key Infrastructure certificate) to every person operating on the department unclassified network. That process is underway for the classified network as well. Department personnel are working with other federal departments and agencies to help them issue the same cyber identity credential to all employees who need to access any of the government's secret networks.
>
> Improving the auditing of information accesses so as to spot anomalous behavior. Department information officers are assessing the use of HBSS and other tools to collect and centralize data about information accesses to more quickly improve detection of malicious insiders.

Though of course, DOD promised to impose some controls on removable media in 2008, when someone introduced malware into DOD's networks via a thumb drive. So after 4 years, DOD should be congratulated for finally closing the Lady Gaga security hole.