ADMIRAL MIKE ROGERS VIRTUALLY CONFIRMS OPM WAS NOT ON COUNTERINTELLIGENCE RADAR

For some time, those following the OPM hack have been asking where the intelligence community's counterintelligence folks were. Were they aware of what a CI bonanza the database would present for foreign governments?

Lawfare's Ben Wittes has been asking it for a while. Ron Wyden got more specific in a letter to the head of the National Counterintelligence and Security Center last month.

1. Did the NCSC identify OPM's security clearance database as a counterintelligence vulnerability prior to these security incidents?
2. Did the NCSC provide OPM with any recommendations to secure this information?
3. At least one official has said that the background investigation information compromised in the second OPM hack included information on individuals as far back as 1985. Has the NCSC evaluated whether the retention requirements for background investigation information should be reduced to

> mitigate the vulnerability of maintaining personal information for a significant period of time? If not, please explain why existing retention periods are necessary?

And Steven Aftergood, analyzing a 2013 Intelligence Community Directive released recently, noted that the OPM database should have been considered a critical counterintelligence asset.

> A critical asset is "Any asset (person, group, relationship, instrument, installation, process, or supply at the disposition of an organization for use in an operational or support role) whose loss or compromise would have a negative impact on the capability of a department or agency to carry out its mission; or may have a negative impact on the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may have a negative impact on the national security of the U.S."
>
> By any reasonable definition, the Office of Personnel Management database of security clearance background investigations for federal employees and contractors that was recently compromised by a foreign adversary would appear to qualify as a "critical asset." But since OPM is not a member or an element of the Intelligence Community, it appears to fall outside the scope of this directive.

But in a private event at the Wilson Center last night, NSA Director Mike Rogers described NSA being brought in to help OPM — but only after

OPM had identified the hack.

> After the intrusion, “as we started more broadly to realize the implications of OPM, to be quite honest, we were starting to work with OPM about how could we apply DOD capability, if that is what you require,” Rogers said at an invitation-only Wilson Center event, referring to his role leading CYBERCOM.
>
> NSA, meanwhile, provided “a significant amount of people and expertise to OPM to try to help them identify what had happened, how it happened and how we should structure the network for the future,” Rogers added.

That “as we started more broadly to realize the implications of OPM” is the real tell, though. It sure sounds like the Chinese were better able to understand the value of a database containing the security clearance portfolios on many government personnel then our own counterintelligence people.

Oops.