NATIONAL COUNTERINTELLIGENCE DIRECTOR EVANINA ABOUT OPM BREACH: "NOT MY JOB"

I've been tracking Ron Wyden's efforts to learn whether the National Counterintelligence and Security Center had anticipated how much of a counterintelligence bonanza the Office of Personnel Management's databases would be. Wyden sent National Counterintelligence Executive William Evanina a set of questions 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?

Evanina just responded. His answer to the first two questions was basically, "Not my job."

> In response to the first two questions, under the statutory structure established by the Federal Information Security Management Act of 2002 (FISMA), as amended, executive branch oversight of agency information security policies and practices rests with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). For agencies with Inspectors General (IG) appointed under the Inspector General Act of 1978 (OPM is one of those agencies), independent annual evaluations of each agency's adherence to the instructions of OMB and DHS are carried out by the agency's IG or an independent external auditor chosen by the agency's IG. These responsibilities are discussed in detail in OMB's most recent annual report to Congress on FISMA implementation. The statutory authorities of the National Counterintelligence Executive, which is part of the NCSC, do not include either identifying information technology (IT) vulnerabilities to agencies or providing recommendations on how to secure their IT systems.

Of course, this doesn't really answer the question, which is whether Evanina — or the NCSC generally — had identified OPM's database full of clearance information as a critical CI asset. Steven Aftergood has argued it should have been, according to the Office of Director of National Intelligence's definition if not bureaucratic

limits. Did the multiple IG reports showing OPM was vulnerable, going back to 2009 and continuing until this year, register on NCSC's radar?

I'm guessing, given Evanina's silence on that issue, the answer is no.

No, the folks in charge of CI didn't notice that this database of millions of clearance holders' records might be a juicy intelligence target. Not his job to notice.

Evanina's response to the third question — whether the government really had to keep records going back to Reagan's second term — was no more satisfying.

> [T]he timelines for retention of personnel security files were established by the National Archives General Records Schedule 18, Item 22 (September 2014). While it is possible that we may incur certain vulnerabilities with the retention of background investigation information over a significant period of time, its retention has value for personnel security purposes. The ability to assess the "whole person" over a long period of time enables security clearance adjudicators to identify and address any issues (personnel security or counterintelligence-related) that may exist or may arise.

In other words, just one paragraph after having said it's not his job to worry about the CI implications of keeping 21 million clearance holders' records in a poorly secured database, the Counterintelligence Executive said the government needed to keep those records (because the government passed a policy deciding they'd keep those just a year ago) for counterintelligence purposes.

In a statement on the response, Wyden, like me, reads it as Evanina insisting this key CI role

is not his job. To which Wyden adds, putting more data in the hands of these insecure agencies under CISA would only exacerbate this problem.

> The OPM breach had a huge counterintelligence impact and the only response by the nation's top counterintelligence officials is to say that it wasn't their job. This is a bureaucratic response to a massive counter-intelligence failure and unworthy of individuals who are being trusted to defend America. While the National Counterintelligence and Security Center shouldn't need to advise agencies on how to improve their IT security, it must identify vulnerabilities so that the relevant agencies can take the necessary steps to secure their data.
>
> The Senate is now trying to respond to the OPM hack by passing a bill that would lead to more personal information being shared with these agencies. The way to improve cybersecurity is to ensure that network owners take responsibility for plugging security holes, not encourage the sharing of personal information with agencies that can't protect it adequately.

Somehow, the government kept a database full of some of its most important secrets on an insecure server, and the guy in charge of counterintelligence can only respond that we had to do that to serve counterintelligence purposes.