THE QUESTIONS THE NCSC DOESN'T WANT TO ANSWER

A few days ago the WaPo published a story on the OPM hack, focusing (as some earlier commentary already has) on the possibility China will alter intelligence records as part of a way to infiltrate agents or increase distrust.

It's notable because it relies on the Director of the National Counterintelligence and Security Center, Bill Evanina. The article first presents his comments about that nightmare scenario — altered records.

> "The breach itself is issue A," said William "Bill" Evanina, director of the federal National Counterintelligence and Security Center. But what the thieves do with the information is another question.
>
> "Certainly we are concerned about the destruction of data versus the theft of data," he said. "It's a different type of bad situation." Destroyed or altered records would make a security clearance hard to keep or get.

And only then relays Evanina's concerns about the more general counterintelligence concerns raised by the heist, that China will use the data to target people for recruitment. Evanina explains he's more worried about those without extensive operational security training than those overseas who have that experience.

> While dangers from the breach for intelligence community workers posted abroad have "the highest risk equation," Evanina said "they also have the best training to prevent nefarious activity against them. It's the individuals who don't have that solid background and

> training that we're most concerned with, initially, to provide them with awareness training of what can happen from a foreign intelligence service to them and what to look out for."
>
> Using stolen personal information to compromise intelligence community members is always a worry.
>
> "That's a concern we take seriously," he said.

Curiously, given his concern about those individuals without a solid CI background, Evanina provides no hint of an answer to the questions posed to him in a Ron Wyden letter last week.

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 has asserted he's particularly worried about the kind of people who would have clearance but not be in one of the better protected (CIA) databases. But was he particularly worried about those people — and therefore OPM's databases — before the hack?