HOW HAL MARTIN STOLE 75% OF NSA'S HACKING TOOLS: NSA FAILED TO IMPLEMENT REQUIRED SECURITY FIXES FOR THREE YEARS AFTER SNOWDEN

The other day, Ellen Nakashima reported that Hal Martin, the Booz Allen contractor who has been in custody for months based on allegations he stole terabytes of NSA's hacking tools, may be indicted this week. The story raises some interesting questions — such as how, absent some proof that Martin leaked this information to a third party, prosecutors intend to distinguish Martin's hoarding from David Petraeus' sharing of code word information with his girlfriend Paula Broadwell. One detail Nakashima included — that Martin had stolen "operational plans against 'a known enemy' of the United States" — may suggest prosecutors plan to insinuate Martin stole the information to alert that known enemy (especially if the known enemy is Russia).

All that said, the detail in Nakashima's story that has attracted the most notice is the claim that Martin stole 75% of NSA's hacking tools.

> Some U.S. officials said that Martin allegedly made off with more than 75 percent of TAO's library of hacking tools — an allegation which, if true, would be a stunning breach of security.

Frankly, this factoid feels a lot like the claim that Edward Snowden stole 1.5 million documents from NSA, a claim invented at least in part because Congress wanted an inflammatory detail they could leak and expand budgets with. That's especially true given that the 75% number comes

from “US officials,” which sometimes include members of Congress or their staffers.

Still, the stat is pretty impressive: even in the wake of the Snowden leak, a contractor was able to walk out the door, over time, with most of NSA’s most dangerous hacking tools.

Except it should in no way be a surprise. Consider what the House Intelligence Report on Snowden revealed, which I mentioned here. Buried way back at the end of the report, it describes how in the wake of Snowden’s leaks, NSA compiled a list of security improvements that would have stopped Snowden, which it dubbed, “Secure the Net.” This initiative included the following, among other things:

- Imposing two person control for transferring data by removable media (making it harder for one individual to put terabytes of data on a thumb drive and walk out the door with it)
- Reducing the number of privileged and authorized data transfer agents (making it easier to track those who could move terabytes of data around)
- Moving towards continuous evaluation model for background investigations (which might reveal that someone had debt problems, as Martin did)

By July 2014, the report reveals, even some of the most simple changes included in the initiative had not been implemented. On August 22, 2016 — nine days after an entity calling itself Shadow Brokers first offered to auction

off what have since been verified as NSA tools — NSA reported that four of the initiatives associated with the Secure the Net remained unfulfilled.

All the while, according to the prosecutors' allegations, Martin continued to walk out of NSA with TAO's hacking tools.

Parallel to NSA's own Secure the Net initiative, in the intelligence authorization for 2016 the House directed the DOD Inspector General to assess NSA's information security. I find it interesting that HPSCI had to order this review and that they asked DOD's IG, not NSA's IG, to do it.

DOD IG issued its report on August 29, 2016, two days after a search of Martin's home had revealed he had taken terabytes of data and the very day he was arrested. The report revealed that NSA needed to do more than its proposed fixes under the Secure the Net initiative. Among the things it discovered, for example, is that NSA did not consistently secure server racks and other sensitive equipment in data centers, and did not extend two-stage authentication controls to all high risk users.

So more than three years after Snowden walked out of the NSA with thousands of documents on a thumb drive, DOD Inspector General discovered that NSA wasn't even securing all its server racks.

"Recent security breaches at NSA underscore the necessity for the agency to improve its security posture," The HPSCI report stated dryly, referring obliquely to Martin and (presumably) another case Nakashima has reported on.

Then the report went on to reveal that CIA didn't even require a physical token for general or privileged users of its enterprise or mission systems.

So yes, it is shocking that a contractor managed to walk out the door with 75% of NSA's hacking tools, whatever that means. But it is also

shocking that even the Edward Snowden breach didn’t lead NSA to implement some really basic security procedures.