WHAT IF THE INSIDER THREAT MEMO IS ABOUT DAVID PETRAEUS?

In a holiday document dump, President Obama transmitted Minimum Standards for Insider Threat Detection Programs. As mere citizens, we don't get to see those standards. We only get to see the memo accompanying them, which leaves us guessing what—if anything—to make of the timing and content of the memo. In addition to Steven Aftergood's general overview, Falguni Sheth, Kevin Gosztola, and Jesselyn Radack have some thoughts.

The simplest explanation for the timing of the memo is that's when the Insider Threat Task Force developing them finished the Standards. The Standards were due a year after Obama ordered the creation of them on October 7, 2011.

> Sec. 6.3. The Task Force's responsibilities shall include the following:
>
> (a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;
>
> (b) **in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch**;

That would mean they were due 45 days before Obama transmitted them. Perhaps the delay can be explained by either the election or a review within the White House (and I'm wonder whether

Obama's victory influenced how Obama received these Standards).

So it could well be that this memo was released as a holiday dump through sheer chance, Obama finishing up business before taking time with the family.

The timing of the transmittal might also be explained by personnel changes. James Clapper and Eric Holder (or their designees) would be the mandatory co-Chairs of the Task Force. While reports suggest Holder will stick around for another year, it's unclear whether Clapper will be.

But then there's the possibility that the Petraeus scandal influenced this release.

As a threshold matter, the EO mandating these Standards includes CIA involvement (by designees of but not the Director himself) on both the Task Force and Steering Committee on Insider Treats. It also reserves the authority of the Director of CIA with regards to security of information systems under an earlier EO and a National Security Directive. What happens where you're in the middle of rolling out an Insider Threat Detection Program and one of the key players involved in it is embroiled in an insider threat investigation himself?

The EO also allows the Director of National Intelligence to "issue policy directives" to help the agencies of the Intelligence Community comply with this.

> With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

Perhaps such "policy directives" no longer seem like such a good idea if the CIA Director can't

even limit his threat profile.

Then there's the possibility that the behavior of one of the players in the scandal demonstrated that the Standards are not yet being met. While reportedly Petraeus and Paula Broadwell only shared a GMail account—and therefore there is no allegation that they used the classified networks addressed in the EO—we have fewer details about what network General Allen was using to exchange sexy-time emails with Jill Kelley. Furthermore, whlie we know Broadwell had classified information on her computer and in her house, we don't have much detail on this, either. As a Reserve Officer, her behavior may well have demonstrated holes in the program implemented by DOD.

In other words, it may be that the Standards had been languishing for 45 days after they were completed, but the Petraeus scandal identified that the Insider Threat Detection *should have* but *did not* identify some of the activities going on. That might have created some urgency for Obama to transmit them, so he could start cracking heads at the agencies where they standards were not being met. Obama's memo also promises the standards will "provide the workforce with insider threat awareness training," so it's possible the Administration believes that if just its top Generals had a bit more training they might not destroy their careers by compromising security. Though, as Marc Ambinder explained, because he was in the chain of command for the nuclear football, Petraeus would have had extensive indoctrination on potential threats.

Or maybe it's something else entirely.

The language used in Obama's memo differs in some interesting ways from the language in the EO on Insider Threats. The latter always refers to agencies, cited back to a 2009 EO …

> (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive

> Order 13526 of December 29, 2009.

Which in turn cites back to laws defining both agencies and departments of the military.

Obama's memo, however, always refers to both agencies and departments:

> This Presidential Memorandum transmits the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) to provide direction and guidance to promote the development of effective insider threat programs within **departments and agencies** to deter, detect, and mitigate actions by employees who may represent a threat to national security.
>
> [snip]
>
> The Minimum Standards provide **departments and agencies** with the minimum elements necessary to establish effective insider threat programs. [my emphasis]

Legally, I suspect there is no difference here, given that agencies as used in the EO includes military departments. But the emphasis seems to be different.

In addition, the EO defines the Insider Threat differently. The EO emphasizes unauthorized disclosure of classified information—the threat identified by WikiLeaks.

> Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, **including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure**, taking into account risk levels, as well as the

> distinct needs, missions, and systems of individual agencies.

But Obama's memo includes "violent acts against the Government."

> These threats encompass potential espionage, **violent acts against the Government or the Nation**, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected United States Government computer networks and systems. [my emphasis]

Mind you, violent acts **should** be included. After all, Nidal Hasan was emailing Anwar al-Awlaki 9 months before he attacked at Fort Hood. And the release of the Webster report provided recommendations that may have been integrated into these Minimum Standards. Plus, given the fearmongering over cyberthreats, Obama may have wanted this out shortly following his EO on cybersecurity.

But again, the emphasis is different.

It may be any of these things: simply the normal timing, the issues others have addressed, real physical threats we may not know about.

But it is, at the very least, ironic that Obama formally implemented these Minimum Standards less than two weeks after two top national security figures were exposed for showing at least bad judgment about their own Insider Threat exposure.