THE NSA'S FUNNY NUMBERS, AGAIN

Back when the WaPo published a quarterly NSA compliance audit from 2012, I caught the largest math organization in the world failing basic arithmetic. I've been comparing that report with the Intelligence Oversight Board report covering the same period, and I'm finding the numbers might, once again, not add up (though it's hard to tell given the redactions).

According to NSA's internal numbers, the organization had 865 violations in the first quarter of calendar year 2012 (670 EO 12333 violations and 195 FISA violations). Yet NSA described just 163 violations in depth (75 EO 12333 violations and 88 FISA violations, though further violations are likely hidden behind redactions in bulk descriptions).

Here's how the numbers compare, broken down by category (I used the categories used in the IOB Report heading, unless the violation was clearly a roamer or a US Person).

Problem	IOB	Audit
Detask/Roamer	32	95
Detask/Other	10	36
Unauthorized Targeting	10	0
Database Queries	2	18
USP	18	17
Other	1	19
Unauthorized Access	8	
Data Handling and Unauthorized Dissemination	7	

Whereas some numbers are very close — such as for the illegal targeting of a US Person — there were other things, such as sharing a US person's data or some fairly troubling unauthorized access violations not explicitly mentioned in the internal audit. Nor are unauthorized targeting and access mentioned as such.

And then there are all the "roamer" incidences, which apparently don't all get reported to IOB (though you can definitely see an increase in them over the years), and which often look a lot less accidental when explained in the IOB

report.

Then there are the rather measured descriptions the NSA gives IOB (which we've seen in other areas, as with the Internet dragnet, and which might be worst with the upstream violations).

Here's what the NSA reported internally:

> As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to document why certain contact chaining rules were created. In addition to the BR work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata.

Here's what NSA told the IOB about this violation:

> [redacted] NSA determined that a technical service contained BR call detail records older than the approved five years. Approximately [redacted] records comprising approximately [fairly big redaction] records were retained for more than five years. The records were found on an access-controlled server that is used exclusively by technical personnel and is not accessible to intelligence analysts. [2 lines redacted]

Here's what PCLOB had to say about this violation:

> In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.

While it appears NSA managed to give IOB (completely redacted) numbers for the files involved, it appears PCLOB never got a clear count of how many were involved. It's not clear that NSA ever admitted this data may have gotten mixed in with Stellar Wind data. No one seems to care that this was a double violation, because techs are supposed to destroy data when they're done with it.

Though, if you ask me, you should wait to figure out why so many records were lying around a tech server before you destroy them all. But I'm kind of touchy that way.

One thing I realize is consistent between the internal audit and the IOB report. The NSA, probably the owner of the most powerful computing power in the world, consistently uses the term "glitch" to describe software that doesn't do what it is designed to to keep people out of data they're not supposed to have access to.

The glitches are letting us down.