LACK OF DUE DILIGENCE: THE NSA'S "THE ANALYST DIDN'T GIVE A FUCK" VIOLATION

The NSA claims there have been no willful violations the law relating to the NSA databases. For example, NSA's Director of Compliance John DeLong just said "NSA has a zero tolerance policy for willful misconduct. None of the incidents were willful." House Intelligence Chair Mike Rogers just said the documents show "no intentional or willful violations."

Which is why I want to look more closely at the user error categories included in the May 3, 2012 audit.

The report doesn't actually break down the root cause of errors across all violations. But it does for 3 different types of overlapping incident types (the 195 FISA authority incidents, the 115 database query ones, and the 772 S2 Directorate violations).

It says the root cause for FISA authority incidents breaks down this way:

- 60 resource (31% of all FISA authority violations)
- 39 lack of due diligence (20% of all FISA authority violations)
- 21 human error (11% of all FISA authority violations)
- 3 training (1.5% of all FISA authority violations)
- 67 system limitations (34% of all FISA authority violations, mostly on the

roamer problem)
- 4 system engineering (2% of all FISA authority violations)
- 1 system disruption (.5% of all FISA authority violations)

It says the root cause of all database query incidents breaks down this way:

- 85 human error (74% of all database query incidents)
- 13 lack of due diligence (11% of all database query incidents)
- 9 training (8% of all database query incidents)
- 7 resources (6% of all database query incidents)
- 1 system disruption (~1% of all database query incidents)

And it breaks down the errors in its worst performing (in terms of violations) Deputy Directorate organization, S2, this way:

- 71 human error (9% of all S2 violations)
- 80 resources (10% of all S2 violations)
- 68 lack of due diligence (9% of all S2 violations)
- 2 resources
- 9 training (1% of all S2 violations)
- 541 system limitations (70% of all S2 violations)

- 1 system engineering

What I'm interested in are the three main types of operator error: human error, resources, and lack of due diligence.

Human error is, from the descriptions, an honest mistake. It includes broad syntax errors, typographical errors, Boolean operator errors, misapplied query technique, incorrect option, unfamiliarity with tool, selector mistypes, incorrect realm, or improper queries. Let's assume, improbably, that none of the violations listed as human error were anything but honest mistakes. These honest mistakes account for anywhere from 9% to 74% of the violations broken out by root cause.

Then there's resource violations. Those are described as "inaccurate of insufficient research information and/or workload issues." So partly, resource violations stem from someone having too much analysis to do. But given that "inaccurate or insufficient research information" always appears first, it seems that resource violations arise when an analyst targets someone based on a faulty understanding about this person. Given how prominent this problem is for FISA violations, I suspect it includes, in part, target location. It may also pertain to targets erroneously believed to have a tie to terror or Chinese military or Iranian nukes. These appear to mistakes based on the analyst not having enough or accurate information before she starts the collection. These may or may not be honest mistakes. The description of them as resource errors suggests they may in part by people taking research short cuts. Resource problems account for anywhere from 6% to 31% of the violations broken out by root cause.

But then there's a third category: lack of due diligence. The report defines lack of due diligence as "a failure to follow standard operating procedures." But some failure to follow standard operating procedure is accounted

for in other categories, like training, the misapplied query techniques, and the apparent inadequate research violations. This category appears to be something different than the "honest mistake" errors categorized under human error. In fact, by the very exclusion of these violations from the "human error" category, NSA seems to be admitting these violations aren't errors. These violations of standard operating procedures, it seems, are intentional. Not errors. Willful violations.

At the very least, this category seems to count the violations on behalf of analysts who just don't give a fuck what he rules are, they're going to ignore the rules.

This category, what consider the "Analyst didn't give a fuck" category, accounts for 9% to 20% of all the violations broken out by root cause.

In aggregate, these violations may not amount to all that many given the thousands of queries run every year — they make up just 68 of the violations in S2, for example. Those 68 due diligence violations make up almost 8% of the violations in the quarter, not counting due diligence violations that may have happened in other Directorates.

John DeLong, who is in charge of compliance at NSA, says the Agency has zero tolerance for willful misconduct. But the NSA appears to have a good deal more tolerance for a lack of due diligence.