

# **WORKING THREAD, INTERNET DRAGNET DUMP 3: EARLY 2009 DOCUMENTS**

This group of documents – all released with this dump – all come from the first couple of months of 2009. The following is my best reconstruction of what they mean; please let me know if you catch any problems with it.

The government noticed Reggie Walton of the “alert function” violation in the phone dragnet on January 15. On January 28, he ordered further reporting on those problems; because he knew the Internet dragnet was similar, he also ordered the government to “determine whether NSA has been processing the electronic communications metadata in accordance with the terms of the Court’s orders.” In response, the government submitted documents M (Government’s Response) and N (Keith Alexander’s declaration), probably on February 15, 2009. While the report claimed (and NSA reported to Congress) only one Internet dragnet practice violated FISC’s orders, there were multiple practices that involved contact chaining beyond two hops, as well as chaining on US persons without First Amendment review. A number of these, however, remain redacted.

As part of report M, the government said it would voluntarily adopt additional oversight mechanisms, as described on page 6-7. One of those mechanisms was an assessment meeting including representatives from DOJ’s National Security Division and NSA’s Office of General Counsel.

Shortly thereafter (I suspect it was after February 25; it may have been between March 5 and March 13, because M and N appear to have been provided to Congress on March 5, the remainder on March 13), the government applied for another Internet dragnet order. That

application consisted of AA (the application), BB (the NSA rep's declaration), and HH (the 90-day report and the NSA/NSD meeting report).

The application reflects several changes from the previous one (see page 3 and 22), all of which reflect changes in response to the early phone and Internet dragnet disclosures. Of particular note, it removed all mention of "archives;" in the phone dragnet and it appears the Internet dragnet, NSA had used "archive" as a gimmick word to allow them to double dip in the dragnet data. In addition, it incorporates the things submitted as voluntary oversight improvements, especially the meeting reported in HH. They also added language about techs accessing the data, language which would change over the year.

The 90-day report was written after Walton started dealing with the violations. For example, it refers to a "broken" process (which happened with one of the phone dragnet fixes; this may have happened on February 20, but will need to double check). Also, it describes the End-to-End report. But it submits several methods of RAS approval (see page 7 of the 90-day report) that had been described in the Alexander declaration that Walton pointedly disapproved in his Primary Order (see page 10).

Walton also added the "additional oversight mechanisms," which the government had presented as voluntary in their February report, as mandatory in his order.

See below the rule for individualized notes.

---

M. Government's Response to a FISC Order February 15, 2009 (probably)

(1) The redacted date is almost certainly January 28, 2009, per this notice to Congress, which also shows this and N have to have been submitted by February 25, 2009.

(2) The reference to "filed this day" is

probably a reference to the report and Alexander declaration dated February 15 (but submitted 2 days later). It is sometimes dated February 12.

(4) This use of chaining to determine a link was noticed in 3 different dockets. I wonder whether it was the most recent 3?

(5-6) This document cites PRTT Primary Order B. But then the additional oversight things appear in the primary order with shall language; this filing says they aren't required. So I'm still not sure which is first.

N. Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director, NSA, Concerning NSA's Compliance with a FISC Order,

(2) The redacted date matches the unredacted January 28 in the BR FISA declaration.

(5) In Hayden's original estimates he said 25% would be USPs. Alexander may be claiming something different in the footnote.

(6) Lying Keith claims words have different meanings from program to program. I'd say there may be reason to doubt him.

(8) I wonder whether the other category referred to in 6 pertains to FISC targets.

(10) Footnote 10 may also pertain to the RAS memo, especially since this is described as a formal guidance.

(12) Only the chaining on 12 got reported as a violation of the Court's orders. But in Primary Order B, Walton seems to shut down all of these. This would suggest B post-dates 2/25, the other practices might have been noticed to Congress.

(13) I think the third report described here would date to around January 2005, though that may be a misinterpretation of what a third report would be.

(16) It's very clear they were chaining on the email side, as they were on the phone side, without First Amendment review.

**AA. Application for Use of Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes,**  
unknown date early 2009

(1) Note they moved application over to NCTC, I guess for the fearmongering

(2) Leiter's statement was filed in an earlier docket. That suggests either they were calling in their fearmongering by this point or this was a reapplication in response to questions Walton raised at the end of the previous docket, as he did with the 08-13 phone dragnet docket at the same time.

(3) Not sure I understand why FBI's investigations are under E0 12333 here.

(3-4) Clearly the application was a response to concerns raised, presumably Walton. It changed in these ways:

- Additional oversight, including a meeting with DOJ.
- Change of key figure to Chief, Oversight and Compliance. The way it's described it sounds like just a change in title.
- Elimination of word "archive." This makes it clear PRTT was doing the same gimmick as the phone dragnet, and makes it clear this post-dated DOJ's admission of that gimmick.
- Inclusion of tech access. At this point this was probably sold as giving techs access to shut down automatic alerts.

(5) Is the redacted phrase after email a description of other things or a novel word for email identifier?

(6) Note footnote 4 which talks about innocent Americans collected, which is redacted.

(7) That the Compliance Chief made this application is one of the things that makes me think it was just a change in title.

(8) David Kris got confirmed NSA AAG later in March, which is why Olsen was on this application – so it happened between January 20 and March 13.

(9) The order seems to parallel the one made in 08-13 docket.

(10) This appears to suggest there were 3 or 4 approved foreign powers.

(12) They still have their fictitious email metadata!!!

(14) The App claims the “NSA exclusively” will operated the data repository. Without help from contractors?

(15) Footnote 9 seems very important. This memo, written after March 2, still only mentions BR FISA, not PRTT. But the problems identifying the data would extend across authorities.

(16) The first redaction seems to suggest the number of analysts has expanded significantly.

(16) Compliance w/the 7/14/04 memo seems like an exceptional request here.

(18) Note that PRTT never got its own set of minimization procedures, like BR FISA did.

(18) Footnote 13 exempts tech people from the minimization procedures.

(20) As with K-K’s order there are clearly other categories besides email.

(21) NSA started aging off data on January 14, just days before the new Administration (and after the BR FISA problems IDed). That was

precisely 4.5 years.

(21) Note the explicit reference to IG. That may support claim that the IG halted its investigation in 2009, not 2011.

**BB. Declaration of NSA Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate.**

(5) Weird language in footnote 2, as if NSA has had approvals on the books for 5 years they never asked for.

(6) Declaration disavows analysis except to make sure they're complying with the orders.

(6) The reference to Tap 1 makes it clear HH was part of this submission.

(21) Remarkable that they're still relying on Hayden's 2004 declaration. On the phone dragnet side, the numbers had changed. Why did they believe they wouldn't on the Internet side?

**HH: Tab 1 Declaration of NSA Chief, Special Oversight and Processing, Oversight and Compliance, Signals Intelligence.**

(3-4) This is precisely the kind of information that, in the phone dragnet, were released. Why not give the real numbers here? It also confirms they were messing with the station table on this side as well.

(4) Phrasing of footnote 3 is interesting;" This process was broken." As if that wasn't the intent.

(4) It looks like the number of email addresses on the station table were in the 5 digit range, which would be consistent with the phone dragnet side. Though the next line looks like 2 more digits!

(5) It looks like they only left one of the ways an email can become RAS approved unredacted.

(6) FISC approved auto-RAS for FISC targets for the phone dragnet in August 2006. Assume it was similar on the Internet side. Wonder why they're

hiding it here? (I also wonder if that's what the RAS memo is?)

(13) The redaction at the bottom of the page may hide discussion of cross-media queries.

(16) Reference to E2E review, and possibly separate audits.

(16) This document appears to post-date EAR. Will try to come back to it but it can be cross referenced with the BR FISA side.

(2) How is it possible the automated query system in BR FISA had not touched the PRTT data? IIRC (again, will check) that was the correlations.

I'm going to assume the Primary Order is next, because it follows directly in the production to Congress, and Document M follows that.

#### **B. PRTT Primary Order, February – March 2009**

The following Primary Order (document C) appears to have been signed May 29. If that's right, this order was probably the first few days of March, 2009.

The typeface of this order matches the 12/12/08 phone dragnet one, but not a 1/28/09 supplement or the 3/5/09 one.

(1) Note this requires application from a designated attorney, with approval from the AG.

(2) The redaction describes the targeting information, which must therefore be more extensive than that in the phone dragnet.

(4) Note the reference to the supplemental opinion.

(5) There's a lot of language that may explain other things the government may get, in addition to the to/from information.

(6) The language on cooperation here is the same used in the assistance of the USA Freedom series of bills. Which makes me wonder whether the government isn't planning in installing

quasi-pen registers.

(7) The CIA was involved in laying out security procedures.

(7) Unlike the phone dragnet, the primary orders could explicitly call for compensation.

(7) The order says data should not be commingled (though there's a footnote). Either this is a new requirement, imposed after the phone dragnet orders, or it was ignored, because we know BR and PRTT data were already lumped together.

(8) Note there's already language for technical access. Walton added that to the phone dragnet side on March 5, 2009.

(9) Unlike the phone dragnet, which just cited the previous docket, this cites 3 in particular.

(9) This permits 23 authorizers for RAS. The 23 authorizers were added on the BR side on April 3, 2008.

(10) The 703/704 language got added to the phone dragnet in September 2008.

(10) The reference to a process being shut down seems to indicate Document HH was part of application that this order approved.

(11) Curiously, these strictures on the access aren't mirrored in the Walton orders from March 2009. They appear to be legacies of the earlier Internet dragnet problems, perhaps dating to the 2004 ones.

(13) Analogues to the paragraphs under (i) were implemented in Walton's September 2009 order (or perhaps earlier—need to double check the summer orders).