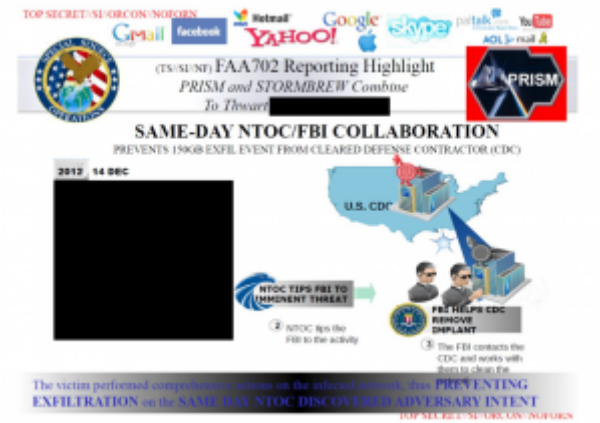
NSA'S SECTION 702 SUCCESS: 150 GIGS OF DEFENSE CONTRACTOR DATA PROTECTED



Over four months ago, I noted that the most impressive success touted in James Clapper's fact sheet on Section 702 pertained to cybersecurity, not terrorism.

> Communications collected under Section 702 have provided significant and unique intelligence regarding potential cyber threats to the United States, including specific potential network computer attacks. This insight has led to successful efforts to mitigate these threats.

Le Monde, as part of its package on US spying on France, published yet another version of the PRISM slide presentation, including this slide (and 2 others that haven't been published before; h/t Koen Rouwhorst).

While I'm not sure we're yet looking at the complete PRISM slideset, at least as it stands, this slide tells the sole success story in the presentation. It describes how, on December 14, 2012, the NSA/CSS Threat Operations Center alerted the FBI to an implant on a Defense contractor's network. The FBI and the contractor managed to take action that same day to prevent

the exfiltration of 150G of data.

And thus using upstream collection (the slide cites Stormbrew), the NSA managed to do something equivalent to stopping China from getting yet another module of data on the F-35 development to go along with all the other data it has stolen.

While I'm glad the NSA prevented yet more tax dollars to be wasted on secrets China (or someone like them) was going to steal anyway, I am rather interested that this gets touted internally as Section 702's big success story.

After all, Keith Alexander has been chanting terror terror terror terror for the last four months. It turns out — as I've been saying all along — it's not about the 54 mostly overseas plots Section 702 has helped to thwart, it's about cybersecurity.

Moreover, it doesn't involve someone's personal communications access via PRISM. It involves upstream collection (this also suggests when NSA describes searching for "selectors" in upstream collection, it searches on more than just emails and phone numbers, as it has previously suggested).

Again, this success is in no way a bad thing—kudos to the NSA for catching this.

It just highlights how we're being sold a dragnet to protect against hackers based on fear of terrorists.

Update: In a Guardian post today, I argue Obama should use the replacement of Keith Alexander as an opportunity to break up NSA.

> Metaphorically, the NSA has pursued its search for intelligence by partly disabling the locks to all our front doors. Having thus left us exposed, it demands the authority to be able to enter our homes to look around and see if those disabled locks have allowed any nasty types to get in.

> Given the way the NSA's data retention procedures have gone beyond the letter of the law to allow them to keep Americans' data if it presents a threat to property (rather than just a threat of bodily harm), while the NSA is looking for nasty types, they might also make sure you don't have any music or movies for which you don't have a receipt. Thus it has happened that, in the name of preventing invaders, the NSA has itself invaded