

# KEITH ALEXANDER: “WE MUST WIN, THERE IS NO SUBSTITUTE FOR VICTORY”

I frankly have no problem with Keith Alexander giving the employees of the National Security Agency a pep talk as the truth of what they’re doing to us becomes public. They are not, after all, responsible for the serial disinformation Alexander and James Clapper have spread about their work. And the overwhelming majority of them are just trying to support the country.

I don’t find this part of Alexander’s speech even remotely accurate, mind you, but I’ve gotten used to dissembling from Alexander.

The issue is one that is partly fueled by **the sensational nature of the leaks and the way their timing has been carefully orchestrated to inflame and embarrass**. The challenge of these leaks is exacerbated by a lack of public understanding of the safeguards in place and little awareness of the outcomes that our authorities yield. Leadership, from the President and others in the Executive Branch to the Congress, is now engaged in a public dialogue to make sure the American public gets the rest of the story while not disclosing details that would further endanger our national security.

It’s hard to understand how leaks can be inflammatory and embarrassing but all the claims about safeguards and dialogue to also be true.

But it’s this passage I’m far more struck by:

Let me say again how proud I am to lead this exceptional workforce, uniformed and civilian, civil service and contract

personnel. Your dedication is unsurpassed, your patriotism unquestioned, and your skills are the envy of the world. **Together with your colleagues in US Cyber Command**, you embody the true meaning of noble intent through your national service. In a 1962 speech to the Corps of Cadets on “**duty, honor and country**,” one of this nation’s military heroes, General Douglas MacArthur, said these words teach us “not to substitute words for action; not to seek the path of comfort, but to face the stress and spur of difficulty and challenge; to learn to stand up in the storm.” You have done all that and more. “Duty, Honor, Country” could easily be your motto, for you live these words every day. [my emphasis]

It’s not just that he calls out Cyber Command in the midst of a scandal that’s not supposed to be (but really is) about offensive war.

It’s not just that he chooses to cite one of the most powerful Generals ever, one who defied civilian command to try to extend a war that – it turns out – wasn’t existential.

But it’s also that he chose to cite a speech that invokes that moment of insubordination, a speech that encourages political inaction among the troops, a speech whose audience MacArthur defined as singularly military.

And through all this welter of change and development your mission remains fixed, determined, inviolable. It is to win our wars. Everything else in your professional career is but corollary to this vital dedication. **All other public purpose, all other public projects, all other public needs, great or small, will find others for their accomplishments;** but you are the ones who are trained to fight.

Yours is the profession of arms, the will to win, the sure knowledge that **in war there is no substitute for victory**, that if you lose, the Nation will be destroyed, that the very obsession of your public service must be Duty, Honor, Country.

**Others will debate the controversial issues, national and international**, which divide men's minds. But serene, calm, aloof, you stand as the Nation's war guardians, as its lifeguards from the raging tides of international conflict, as its gladiators in the arena of battle. For a century and a half you have defended, guarded and protected its hallowed traditions of liberty and freedom, of right and justice.

**Let civilian voices argue the merits or demerits of our processes of government.** Whether our strength is being sapped by deficit financing indulged in too long, by federal paternalism grown too mighty, by power groups grown too arrogant, by politics grown too corrupt, by crime grown too rampant, by morals grown too low, by taxes grown too high, by extremists grown too violent; whether our personal liberties are as firm and complete as they should be.

**These great national problems are not for your professional participation or military solution.** Your guidepost stands out like a tenfold beacon in the night: Duty, Honor, Country.

At a moment of crisis, at a moment when his own credibility is under strain, Keith Alexander has chosen to address the military, civilian, and contractor employees of the NSA as unthinking warriors, isolated from the critical issues swirling around them at the moment. He has chosen to frame NSA as a war machine, not as a defense machine.

The employees of NSA's first duty is to the Constitution, not the secret battles Alexander wants to escalate and win at all costs. I do hope they don't despair of that duty.

---

## **SHORTER WAPO: IT WOULD TAKE MONTHS TO KNOW ABOUT SPYING MISCONDUCT**

For what it's worth, I consider reports that the government doesn't know what Edward Snowden took to be disinformation. And indeed, claims to that effect in this WaPo article are sourced to: "one former government official," a "former senior U.S. official," and "a former senior U.S. intelligence official who served in Russia." There's also "a senior intelligence official" who says only it'll take months to complete the damage assessment on Snowden's materials, which is different from claiming (as the other sources do) that Russia and China have what he took. And a "second senior intelligence official" who fearmongers improbably about how much easier this will make things on the terrorists.

But ultimately, most of the people claiming NSA doesn't know what Snowden took are former officials, presumably out of the loop on such issues (unless, of course, they're Booz Allen Hamilton revolving doormen).

Funny thing is, if all that were true – if the government is still struggling to figure out what Snowden took a month after he left NSA – it indicates that the government would not know if a Sysadmin at the NSA had spied on Americans, if ever, until months after someone did so.

But, promise, this giant dragnet is secure.

Update: Mark Hosenball's version of this apparently organized leak (his is sourced to "several U.S. officials," "one non-government source familiar with Snowden's materials," and "2 U.S. national security sources," makes it fairly clear the government intends to release this disinformation – along with incorrect claims about the history of WikiLeaks – as a way to fearmonger about that connection.

Although WikiLeaks initially made the diplomatic cables available to media outlets, including the Guardian and New York Times, who redacted potentially sensitive information before publishing them, the website eventually released an entirely unredacted archive of the material, to the dismay of the Obama Administration. U.S. officials said the information put sources at risk and damaged relations with foreign governments.

The disinformation people spreading this story apparently are less worried about confirming genuine concerns about the security of these programs than they are about trying to catch up to WikiLeaks involvement with a new line of fearmongering.

Update: I changed the title of this after it was published.

---

## **OBAMA'S STUBBORNNESS AND THE RISK OF SNOWDEN**

At the outset of this post, let me lay out my following assumptions (I can't prove these points, but I suspect them):

- The documents released so far by Guardian and WaPo – information on the Section 215 program, PRISM, and the PPD on cyberwar – have done negligible damage to our security (indeed, even Sheldon Whitehouse, a big defender of these programs, said the government should have been transparent about them earlier)
- China already knew the content of Edward Snowden's public revelations about our hacking into Chinese networks (we know China's compromises of us, so it is unlikely China, which is more successful and aggressive at hacking than we are, doesn't know our compromises of it); the revelations on this front so far have served primarily to even out the playing field on mutual accusations of hacking
- Snowden personally (and his laptops) have information that China and Russia could both find of more use, particularly given that some of our programs targeting them were run out of HI
- Snowden may also have things that might be of use to

others, such as organized crime (If I were planning on longevity and had access, for example, I would take some zero day exploits when I left the NSA, though the street value of them would diminish once NSA had inventoried what I took)

- The reporting I've seen has not confirmed reports that either China or Russia has debriefed Snowden or scanned his computers (indeed, this report on China's involvement in his departure from Hong Kong suggests they did not talk with him directly)
- Julian Assange knows where Snowden is, leading to the possibility he has escaped Russia to a country that has not yet been named in reports of Snowden's escape (named countries have included Venezuela, Cuba, Ecuador, and Iceland)

All of that is a roundabout way of saying that Snowden could do great damage to the US, but may not have yet, and certainly hadn't by the time he first revealed himself in Hong Kong.

If that's right, then it seems the Obama approach has been precisely the wrong approach in limiting potential damage to national security. The best way to limit damage, for example, would be to get Snowden to a safe place where our greatest adversaries can't get to him,

where we could make an eternal stink about his asylum there, but still rest easy knowing he wasn't leaking further secrets. Indeed, if he were exiled in some place like France, we'd likely have more influence over what he was allowed to do than if he gets to Ecuador, for example.

The most likely approach to lead to further damage, however, is to charge him with Espionage. This not only raises the specter of the treatment we've given Bradley Manning – giving Snowden Denise Lind's judgement that Manning's rights were violated to include in any asylum application – but also easily falls under what states can call political crimes, which permits them to ignore extradition requests. That is, we appear to be pursuing the approach that could lead to greater damage.

By contrast, letting Snowden get someplace safe is perfectly equivalent to letting the CIA off for torture (or, for that matter, James Clapper off for lying to Congress). It's a violation of rule of law, but it also serves to minimize the tremendous damage the spooks might do to retaliate. Obama has chosen this path already when the criminals were his criminals; he clearly doesn't have the least bit of compunction of setting aside rule of law for pragmatic reasons. But in Snowden's case, he seems to be pursuing a strategy that not only might increase the likelihood of damage, but also lets China and Russia retaliate for perceived slights along the way.

All this is just an observation. I believe Obama's relentless attacks on whistleblowers and his ruthless enforcement of information asymmetry have actually raised the risk of something like this. And he seems to be prioritizing proving the power of the US (which has, thus far, only proved our diminishing influence) over limiting damage Snowden might do.

Update: This fearmongering WaPo article nevertheless quotes a former senior US official



admitting that what Snowden has released so far wouldn't help China or Russia.

A former senior U.S. official said that the material that has leaked publicly would be of limited use to China or Russia but that if Snowden also stole files that outline U.S. cyber-penetration efforts, the damage of any disclosure would be multiplied.

---

## KEITH ALEXANDER'S “PACKETS IN FLIGHT” TURN HACKERS INTO TERRORISTS

Keith Alexander showed up to chat with a typically solicitous George Stephanopoulos yesterday. The interview demonstrates something I'll be increasingly obsessed with in upcoming weeks.

The government is using the limited success of NSA's counterterrorism spying to justify programs that increasingly serve a cybersecurity function – a function Congress has not enthusiastically endorsed.

The interview starts with Alexander ignoring Steph's first question (why we didn't find Snowden) and instead teeing up 9/11 and terror terror terror.

And when you think about what our mission is, I want to jump into that, because I think it reflect on the question you're asking.

You know, my first responsibility to the American people is to defend this nation. And when you think about it,

defending the nation, let's look back at 9/11 and what happened.

The intel community failed to connect the dots in 9/11. And much of what we've done since then were to give us the capabilities – and this is the business record FISA, what's sometimes called Section 215 and the FAA 702 – two capabilities that help us connect the dots.

The reason I bring that up is that these are two of the most important things from my perspective that helps us understand what terrorists are trying to do. And if you think about that, what Snowden has revealed has caused irreversible and significant damage to our country and to our allies.

When – on Friday, we pushed a Congress over 50 cases where these contributed to the understanding and, in many cases, disruptions of terrorist plots.

Steph persists with his original question and gets Alexander to repeat that they've "changed the passwords" at NSA to prevent others from leaking.

Steph then asks Alexander about Snowden's leaks of details on our hacking of China (note, no one seems to be interested in this article, which is just as revealing about our hacking of China as Snowden's revelations).

Note how, even here, Alexander says our intelligence collection in China is about terrorism.

STEPHANPOULOS: In the statement that Hong Kong put out this morning, explaining why they allowed Snowden to leave, they also say they've written to the United States government requesting clarification on the reports, based on Snowden's information, that the United

States government attacked (ph) computer systems in Hong Kong.

He said that the NSA does all kinds of things like hack Chinese cell phone companies to steal all of your SMS data.

Is that true?

ALEXANDER: Well, we have interest in those who collect on us as an intelligence agency. But to say that we're willfully just collecting all sorts of data would give you the impression that we're just trying to canvas the whole world.

The fact is what we're trying to do is get the information our nation needs, the foreign intelligence, that primary mission, **in this case and the case that Snowden has brought up is in defending this nation from a terrorist attack.**

Alexander then shifts the issue and suggests we're collecting on China because it is collecting on us.

Now we have other intelligence interests just like other nations do. That's what you'd expect us to do. We do that right. Our main interest: who's collecting on us?

Alexander next goes on to answer Steph's question about whether we broke Hong Kong law by saying this hacking doesn't break our law. He also says he doesn't "track" WikiLeaks, but knows who Julian Assange is, which I take to be confirmation NSA targets Assange and collects on everyone else he talks to.

Then Steph tees up the 50 plots prevented, without noting that, of the four publicly released, there are major holes in the claims made about the three most serious plots. He asks for proof in these cases and Alexander provides nothing new (indeed, he actually comes close to

admitting that the FISA programs played just a role in connecting the dots).

After letting Alexander continue on about these 50 plots for over 400 words, he moves onto challenging, sort of, the claims that the US can't listen into an American side of a conversation. Interestingly, Steph asks about Cuba, but Alexander responds by focusing on terrorism. Again.

But is that statement correct? I would assume – and tell me if I'm wrong here, that if the NSA (inaudible) tracking someone, say, in Cuba or someone overseas, who then calls the United States, you're going to listen to that phone call, correct?

ALEXANDER: Right. You're asking a different set of questions.

So let me put, first of all, the prime directive on the table. The FISA law makes it clear: in order for the NSA to target the content of a U.S. persons communications, anywhere in the world – anywhere – NSA requires probable cause and a court order, a specific court order.

So if we're targeting outside the U.S. a terrorist, and they happen to talk to a U.S. person inside the United States, yes, we would follow that law.

Alexander doesn't address Steph's question (he says the NSA abides by minimization rules, which do permit accessing the US person side of the call), but he does use the word "target" a lot.

And then, having not mentioned FAA's role in cybersecurity during this entire extended debate about it, Steph switches to Alexander's role in cyberwar, asking about NSA's pre-emptive strike ability. This is where Alexander raises his authority to "stop packets in flight" as parallel to a nuclear assault.

ALEXANDER: So to be clear, what I can do on my own right now is within our networks to launch offensive measures to stop somebody from getting into the networks.

Anything that I want to do outside the networks that is offensive in nature, we would have to call the secretary and the president to get their approval.

So there are things that we can do to **stop packets in flight**. But from our perspective, any actions that's offensive in nature would require the policymakers. This is no different than if you think about the **nuclear situation**. [my emphasis]

Steph ends the interview by teasing up one of Alexander's (and Sheldon Whitehouse's) favorite claims about cybersecurity, that it represents a transfer of wealth greater than slavery or colonization did.

STEPHANOPOULOS: Finally, the chairman of the House Intelligence Committee, Mike Rogers, was on this program a short while ago. And he said we're losing the cyber war to China.

Is he right?

ALEXANDER: Well, I think our nation has been significantly impacted with intellectual property, the theft of intellectual property by China and others. That is the most significant transfer of wealth in history.

And it goes right back to your initial question: who's taking our information? Is one of the things I believe the American people would expect me to know. That's one of my missions. Who's doing this to us? And why?

So when you asked your initial question, why, there's part of the answer. Who's

coming after us? We need to know that so we can defend this nation.

It's the greatest transfer of wealth in history, Alexander lies, but he still doesn't admit in this entire interview that FAA also serves a key role in cybersecurity.

As I said, I will be increasingly obsessed with this in upcoming weeks. The government is hiding its use of these newly exposed authorities behind a lot of fearmongering about terrorism.

And Keith Alexander was so intent on maintaining that approach he even accused China of terrorism.

---

## WHO ARE THE POTENTIAL TARGETS OF THE OTHER SECTION 215 PROGRAM(S)

There are several small, but significant, discrepancies between what Dianne Feinstein and Keith Alexander said in yesterday's Senate Appropriation Committee hearing on cyber and what others have said. As one example, last week James Clapper said this was the standard for accessing the dragnet of Americans' call data:

The court only allows the data to be queried when there is a reasonable suspicion, **based on specific facts**, that the particular basis for the query is associated with a foreign terrorist organization. [my emphasis]

DiFi yesterday said this was the standard:

It can only look at that data after a

showing that there is a reasonable, **articulable suspicion** that a specific individual is involved in terrorism, actually **related to al Qaeda or Iran**.  
[my emphasis]

These are slightly different things (and Congress has fought hard over the word “articulable” in very similar contexts to this in the past – plus, whichever word is used may trace back to Jack Goldsmith’s 2004 OLC opinion on the illegal wiretap program). It’s possible – likely even – that Clapper was just dumbing down his statement the other day. But it is a difference.

I’m particularly interested in the point I raised yesterday. DiFi, in discussing the NSA’s use of the Section 215 data, says it can only be used to find people in the US with ties to terrorists or Iran.

But when Clapper discussed all the potential targets the Intelligence Community might want to trace using Section 215 data, he mentioned a broader group.

There are no limitations on the customers who can use this library. Many and millions of innocent people doing min– millions of innocent things use this library, but there are also nefarious people who use it. **Terrorists, drug cartels, human traffickers, criminals** also take advantage of the same technology. So the task for us in the interest of preserving security and preserving civil liberties and privacy is to be as precise as we possibly can be when we go in that library and look for the books that we need to open up and actually read. [my emphasis]

But remember. Clapper oversees all 16 members of the intelligence community, including FBI and the National Counterterrorism Center. DiFi’s

statement (and Alexander's confirmation) applied only to NSA. Elsewhere in the hearing, Alexander said NSA only used what he called "BR" (for business records) to collect phone records. And we know that – at least as recently as 2011 – there was at least one other secret collection program using Section 215. So one of those other entities – almost certainly FBI – must run that program.

Moreover, there's no reason to believe that Edward Snowden, who had unbelievable access to NSA's networks and, some time ago, CIA's records, would have access to programs that didn't involve those agencies.

And Keith Alexander probably knows that.

Also, terrorists, certainly, and Iran, sort of, are legitimate targets for DOD (I'm actually wondering if the government has acrobatically justified going after Iranian contacts by relying on the still extant Iraq AUMF). For NSA to pursue drug cartels and criminals might present a posse comitatus problem (one that I believe was part of the problem behind the 2004 hospital confrontation).

So I'm wondering how many of the answers we're getting are designed to minimize the scope of what we know by referring only to the NSA programs?

---

**IF WANTING TO REVEAL  
THAT ALL AMERICANS'  
METADATA GETS SWEEP  
UP IS TREASON,**



# EDWARD SNOWDEN IS IN DISTINGUISHED COMPANY

Earlier this evening, Dianne Feinstein called Edward Snowden's decision to leak NSA documents an act of treason.

"I don't look at this as being a whistleblower. I think it's an act of treason," the chairwoman of the Senate Intelligence Committee told reporters.

The California lawmaker went on to say that Snowden had violated his oath to defend the Constitution.

"He violated the oath, he violated the law. It's treason."

Perhaps DiFi can be excused for her harsh judgment. After all, in addition to exposing the sheer range of surveillance our government is doing, Snowden made it very clear that DiFi allowed Director of National Intelligence James Clapper to lie to her committee.

And continues to allow Clapper's lie to go unreported, much less punished.

But I thought it worthwhile to point out the many people who have committed to make the FISA Court Opinions describing, among other things, how the government's abuse of Section 215 violated the Constitution.

In 2010, DOJ promised to try to declassify important rulings of law.

In 2010, as part of the same effort, Clapper's office promised to try to declassify important rulings of law.

In 2011, prior to be confirmed as Assistant Attorney General, now White House Homeland Security Advisor Lisa Monaco promised, "I will work to ensure that the Department continues to

work with the ODNI to make this important body of law as accessible as possible.”

All these people claimed they wanted to make FISC’s opinion, among other things, on the secret use of Section 215 public.

What Snowden released on Section 215 – just a single 215 order to Verizon, without details on how this information is used – is far, far less than what DOJ and ODNI and Lisa Monaco pledged to try to release. Given that the collection is targeted on every single American indiscriminately, it won’t tell the bad guys anything (except that they’ve been sucked into the same dragnet the rest of us have). And while it shows that FBI submits the order but the data gets delivered to NSA (which has some interesting implications), that’s a source and method to game the law, not the source or method used to identify terrorists.

So if Snowden committed treason, he did so doing far less than top members of our National Security establishment promised to do.

Wait.

There’s one more member of this gang of – according to DiFi – **traitors** committed to tell Americans how their government spies on them. There’s the Senator who said this on December 27, 2012.

I have offered to Senator *Merkley* to write a letter requesting declassification of more FISA Court opinions. If the letter does not work, we will do another intelligence authorization bill next year, and we can discuss what can be added to that bill on this issue.

Oh, wait! That was Senator Dianne Feinstein, arguing that they didn’t have time to pass an actual amendment, attached to the actual FISA Amendments Act renewal, forcing the government to turn over this secret law.

**But she promised to write a letter!**

And even, DiFi claimed (though similar promises to John Cornyn to obtain the OLC memo authorizing Anwar al-Awlaki's killing went undelivered), to include a requirement in this year's intelligence authorization requiring the government to turn over far more information on the government's use of Section 215 than Snowden did.

I get that DiFi doesn't agree with his method – that he leaked this rather than (!) write a letter. I get that Snowden has exposed DiFi for allowing Clapper lie to her committee, in part to hide precisely this information.

But in debates in the Senate, at least, DiFi has claimed to support releasing just this kind of information.

---

## **JAMES CLAPPER HAILS CHECKS AND BALANCES WHILE TREATING OVERSIGHT “TOO CUTE BY HALF”**

I've been citing bits of this interview between James Clapper and Andrea Mitchell here and there, but the whole thing needs to be read to be believed.

But the quick version is this. Mitchell asks Clapper whether “trust us” is enough, given that some future President or Director of National Intelligence might decide to abuse all the programs in question. Clapper responds by celebrating our constitutional system's checks and balances.

ANDREA MITCHELL:

The president and you and the others in this top-secret world, are saying, "Trust us. We have your best interests, we're not invading your privacy, we're going after bad guys. We're not going after your personal lives." What happens when you're gone, when this president or others in our government are gone? **There could be another White House that breaks the law.**

There could be another D.N.I. who does really bad things— we listened during the Watergate years to those tapes. With the President of the United States saying, "Fire bomb the Brookings Institution." You know, what do you say to the American people about the next regime who has all of these secrets? Do they— do they live forever somewhere in a computer?

JAMES CLAPPER:

No, they don't live forever. That's a valid concern, I think. You know, people come and go, presidents come and go, administrations come and go, D.N.I.'s will come and go. But **what is, I think— important about our system is our system of laws, our checks and balances.**

You know, the— I think the founding fathers would actually be pretty impressed with how— what they wrote and the organizing principles for this country are still valid and are still used even in you— to— to regulate a technology then, they never foresaw. So that's timeless. That— those are part of our institutions. Are there people that will abuse those institutions? Yes. But we have a system that sooner or later, mostly sooner these days, those misdeeds are found out. [my emphasis]

But when, earlier in the interview, Mitchell asks him about his lie to Ron Wyden, here's how he answered.

ANDREA MITCHELL:

Senator Wyden made quite a lot out of your exchange with him last March during the hearings. Can you explain what you meant when you said that there was not data collection on millions of Americans?

JAMES CLAPPER:

First— as I said, I have great respect for Senator Wyden. **I thought, though in retrospect, I was asked— “When are you going to start— stop beating your wife” kind of question, which is meaning not— answerable necessarily by a simple yes or no.** So I responded in what I thought was the most truthful, or least untruthful manner by saying no.

And again, to go back to my metaphor. What I was thinking of is looking at the Dewey Decimal numbers— of those books in that metaphorical library— to me, collection of U.S. persons' data would mean taking the book off the shelf and opening it up and reading it.

ANDREA MITCHELL:

Taking the contents?

JAMES CLAPPER:

Exactly. That's what I meant. Now—

ANDREA MITCHELL:

You did not mean archiving the telephone numbers?

JAMES CLAPPER:

No.

ANDREA MITCHELL:

Let me ask you about the content—

JAMES CLAPPER:

And this has to do with of course somewhat of a semantic, perhaps some would say too— **too cute by half**. But it is— there are honest differences on the semantics of what— when someone says “collection” to me, that has a specific meaning, which may have a different meaning to him. [my emphasis]

I’m grateful that Clapper himself describes this ploy as “too cute by half,” because I’ve been struggling for a description that didn’t involve potty mouth words.

Nevertheless, the semantics at issue have nothing to do with the word “collection” (except in a way I’ll describe in a follow-up post). Rather, it has to do with the definition of “data.” Elsewhere, Clapper is clinging to the fact that the Section 215 er, um, collection involves “just metadata.” And yet here, when asked specifically about “any type of data,” Clapper pretended that data meant content.

Mitchell then went on to ask Clapper about whether the rest of Congress had been adequately informed about the NSA programs, and he responded, in part, by pointing the important role the Intelligence Committees serve in that process.

ANDREA MITCHELL:

Do they— do they know what they’re voting on?

JAMES CLAPPER:

I— I trust so. Obviously, our primary congressional interlocutors are— are two Intelligence Oversight Committees, both in the House and the Senate.

Remember, he has just said that he treats the Intelligence Committees, his primary congressional interlocutors, as “too cute by

half.”

Which brings us to the point, much later in the interview, when the man who explains away his lies to his primary interlocutors in Congress as “too cute by half” semantics, admits how important personal trust is to keeping secrets.

ANDREA MITCHELL:

And are new procedures being put in to try to protect against this flow of leaks?

JAMES CLAPPER:

Well, we’ve— we’re constantly trying to institute new procedures. I’m in the process of attempting to institute some practices and policies that will try to stem the hemorrhage of— leaks, leaking that we’ve— we’ve had in recent years. But this is a tough problem because when it boils down to it, we operate, even though we have clearances and we have skiffs and— and secure areas, when it all boils down to it, it’s all about personal trust.

And we’ve had violations of that personal trust in the past and we will continue to have them. And all we can do is learn lessons from what we— when we find out what caused— a revelation like this and make improvements and go on.

James Clapper, who has treated an important check on his power as “too cute by half”—and with it, effectively misinformed Congress and the American people, making it impossible for elections to serve as another of those checks our founders laid out—now wonders why someone violates the personal trust of a security agreement.

Congress, especially the members of the Intelligence and Judiciary Committees who have voted against key limits on these powers, are clearly complicit in these programs.

But before you even get there, you're at the point where Executive Branch officials have bypassed the checks and balances of our Constitution by engaging – by James Clapper's own admission! – in “too cute by half” semantic games to keep Congress and the public misinformed.

Well before you get to the violation of the personal trust of a security clearance, you've got these lies masquerading as cute semantics. No wonder we have leaks.

---

## **DOD INSPECTOR GENERAL REPORT: SOCOM PURGED THEIR OSAMA BIN LADEN FILES AFTER JUDICIAL WATCH FOIA**

I wanted to point to one more detail from the DOD Inspector General's report on Leon Panetta's leaks to Zero Dark 30's filmmakers.

The very last page of the report describes how Admiral William McRaven responded after realizing the SEALs who had participated in the raid on Osama bin Laden's compound had all hung around a Hollywood producer with their name badges exposed.

According to ADM McRaven, the DoD provided the operators and their families an inordinate level of security. ADM McRaven held a meeting with the families to discuss force protection measures and tell the families that additional protective monitoring will be provided, and to call



security personnel if they sensed anything. ADM McRaven **also directed** that the names and photographs associated with the raid not be released. **This effort included purging these records** to another Government Agency. [my emphasis]

The report doesn't reveal when SOCOM purged its records and handed the documents to, presumably though not definitely, CIA, though if McRaven directed it, it happened after he took command in August 2011. (Update: That's probably not right, as he was in command of the operation in any case.)

But it's a relevant question because Judicial Watch had FOIAed pictures of OBL on May 3, 2011, and sued 10 days later, so before all the leaking and presumably therefore the purging began. On June 26, 2011, just two days after Panetta's leaky party, the government stalled on the suit, saying Judicial Watch had not exhausted its administrative remedies. By September 26, DOD claimed they had no pictures of OBL (though earlier this year there were reports 7 new photos had been found) and CIA claimed none of the 52 pictures they had could be released. Along with that filing, McRaven submitted a declaration explaining why these photos couldn't be released, though the interesting parts remain redacted. John Bennett's declaration for the CIA does not describe when the Agency searched its files for photographs, and therefore doesn't indicate whether they searched before or after DOD purged its files.

Now, none of this timing would mitigate CIA's claims about the extremely grave harm that would arise from releasing OBL death porn.

But it is, at the very least, very sketchy – and all that's before having a really good sense of when the purging and the FOIA response occurred.

Update: I spoke to Judicial Watch's lawyer for this FOIA, Michael Bekesha, and they have never

been informed of this purge. Though it may explain some other details about the progress of the FOIA, including some funkiness with the classification of the photos.

Update: Here's DOD's declaration about their search from September 26, 2011.

It's interesting for two reasons. First, they make claims about SOCOM files that is the exact opposite of what DOD said in the NYT/ACLU FOIA for Anwar al-Awlaki related OLC memos. Whereas in the drone FOIA, they claimed CENTCOM handled SOCOM's FOIA responses, this one says,

The mission of USSOCOM is to provide Special Operations Forces to defend the United States and its interests. A priority of USSOCOM is to "Deter, Disrupt, and Defeat Terrorist Threats," and a primary aspect of this priority is to plan and conduct special operations. When a special operation is conducted, the military service Components of USSOCOM (U.S. Army Special Operations Command, Navy Special Warfare Command, U.S. Air Force Special Operations Command, and Marine Corps Special Operations Command) provide Special Operations Forces (personnel and equipment) to the operation. Accordingly, it is DoD FOIA policy that documents created or maintained by these military service Components during or for a joint special operation come under the cognizance of USSOCOM and not the military services for purposes of the FOIA. Therefore, USSOCOM and not the military services, is responsible for the searches of records responsive to plaintiff's FOIA request at those service components that may have participated in the subject operation.

And like CIA, they don't date their search description at SOCOM, so don't say whether it happened pre- or post-purge.

USSOCOM searched the Headquarters and relevant Components, and no records responsive to plaintiff's request were located. The specific filing systems searched at the Headquarters USSOCOM offices and relevant Components were all hard copy and electronic records including all email records during the inclusive dates of May 1, 2011, through May 31, 2011.

---

## **AL PACINO COULDN'T PROTECT CIA HEADQUARTERS**

There's a funny passage from the DOD Inspector General on Leon Panetta's blabbing about the Osama bin Laden raid that was leaked to POGO.

It describes CIA's apparent helplessness from protecting CIA Headquarters from being breached by outsiders, even while many of our nation's most elite warriors were present.

In a description of how a Hollywood Executive (possibly Kathryn Bigelow) managed to attend a celebration of the successful Osama bin Laden raid, the report explains,

On June 24, 2011, the CIA held an awards ceremony in a tent located on the grounds of the CIA headquarters. Two to four days prior to this awards ceremony, a CIA [Public Affairs Officer] contacted a DoD PAO to notify the DoD PAO that one of the Hollywood executives may attend the event. According to the DoD PAO, the CIA PAO attempted to prevent this from happening. The DoD PAO did not inform his Chain of Command or the special operators who were going to attend this

ceremony about the possibility that a Hollywood executive might also attend. The DoD PAO said he did not forward this information because he hoped the CIA PaO would be able to ensure the Hollywood executive would be refused access. The DoD PAO's current Deputy Commanding General told us he knew of those DoD PAO actions and did not fault the DoD PAO for not getting the information to the command group.

According to the DoD PAO, the day of the event, the CIA PAO contacted the DoD PAO to state that efforts failed and the "Chief of Staff" directed that the Hollywood executive be given access to the event.

It seems that Leon Panetta's Chief of Staff, Jeremy Bash, and CIA's Public Affairs Officer disputed who let the crafty Hollywood executive breach the nation's premier spy agency. But breach Langley he or she did.

Mind you, all this went down a month before Pentagon Press Secretary George Little revealed that Panetta wanted Al Pacino to play him in Zero Dark 30.

Mr. Little: "I hope they get Pacino to play [Secretary Panetta]. That's what he wants, no joke!"

Nevertheless, the lesson from this sordid tale appears to be that if terrorists want to breach CIA Headquarters, all they have to do is dangle the name of a famous actor who might play the part of the CIA Director, and they'll walk into the middle of a highly classified party, even as Osama bin Laden's killers prowl the site.

This must be what Obama means when he claims to run the most Transparent Administration Ever™.

---

# LEON PANETTA: SHEEP DIPPING SECRETS

POGO has a story that adds a new twist to an old story.

The old story is Leon Panetta, leaking classified info, in this case, leaking info on the Osama bin Laden raid to a Zero Dark Thirty executive.

In June 2011, when he was director of the Central Intelligence Agency, Panetta discussed the information at a CIA headquarters event honoring participants in the raid that killed Osama bin Laden, according to an unreleased report drafted by the Inspector General's office and obtained by the Project On Government Oversight (POGO).

"During this awards ceremony, Director Panetta specifically recognized the unit that conducted the raid and identified the ground commander by name," the draft report says. "According to the DoD Office of Security Review, the individual's name is protected from public release" under federal law, the report says.

"Director Panetta also provided DoD information, identified by relevant Original Classification Authorities as TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL, as well as, SECRET/ACCM," the report says.

This is the investigation Peter King requested in 2011.

The new, but predictable, twist, is that when DOD's Inspector General tried to investigate

this, it apparently got no cooperation from Panetta himself, who had subsequently moved over to head DOD itself. More importantly, the IG stalled the report, apparently until Panetta retired.

The unknown fate of the IG report was the subject of a December 2012 email exchange—obtained by POGO—between a congressional staff member and an employee in the IG’s office. The congressional aide mentions having heard that someone in the IG’s office was “sitting on it until Secretary Panetta retires” and asks the IG employee for any information about it.

The IG employee replies: “That effort . . . has been controlled and manipulated since inception by the IG Front Office.” The employee adds: “There is a version ready to hit the street, been long time ready to hit the street...but we will see if that happens anytime soon. Highly unusual tight controls and tactical involvement from senior leadership on this project.”

The employee says the matter reflects broader problems within the IG’s office.

“I have grave concerns that the message and findings are now controlled and subject to undue influence across the board at DoD IG. I have never experienced or seen so much influence or involvement by outsiders now in developing and issuing oversight reports.”

The IG employee invokes whistleblower status.

“I consider this protected communications on alleged wrong-doings within the Government.”

While it doesn’t say so directly, POGO suggests

the Obama Administration may have pulled this off by withholding the nomination for the Acting Inspector General to become its permanent IG.

The Defense Department IG's job has been vacant since December 2011, and the office has been headed on a temporary basis by Lynne M. Halbrooks, who is now the principal deputy inspector general. She has sought support to be named permanent inspector general, a presidential appointment that traditionally involves the approval of the secretary.

In short, Panetta exposed a classified identity to a movie maker, as well as SIGINT pertaining to the Osama bin Laden raid (perhaps reports on the intercepts the government used to identify the courier?). But rather than being treated like John Kiriakou, for example, Panetta got moved into a position to prevent any release of this information.

The term "sheep dip" has been adopted to refer to the practice of having Special Forces operate under CIA guise, as they did on this OBL raid, to operate under CIA's covert authorities. It turns out the institutional shell game with the OBL raid served not to keep secrets, nor even to sustain deniability from the Pakistanis (particularly after Panetta identified Shakeel Afridi), but rather to allow the Administration to treat this covert operation just like they do covert operations like drones (Joby Warrick's book, *The Triple Agent*, includes a lot on drones that obviously comes from Panetta's office too), to make them selectively public.