

# GOVERNMENT SPYING: WHY YOU CAN'T 'JUST TRUST US'



Okay you Wheelhouse mopes, Marcy, Jim and I are all in San Jose at Netroots. Not sure the jail in this here town is big enough to hold us all. Marcy already put up two posts earlier today, but posting may

be a bit spotty, we shall see. I have an important one that will probably go up tomorrow morning on the Aaron Swartz case.

At any rate, to give some extra fodder here, and because Ms. Wheeler is terminally lame at noticing our own blog when she writes articles elsewhere, I am hereby placing you on notice that she has a great article that went up late yesterday at The Nation titled:

Government Spying: Why You Can't 'Just Trust Us'

Go read it, you will be glad you did! Other than that, use this as an open thread for Trash Talk (GO SPURS!), and anything and everything else you want to yammer about.

---

## COMMISSARY CHEAP

Most of the veterans I follow on Twitter are pointing to this WaPo story on DOD's failure to eliminate commissaries on bases as an example of the worst of DOD bureaucracy.

Three summers ago, Richard V. Spencer, a retired investment banker who serves on a Pentagon advisory board, proposed

shutting down the commissary at Camp Lejeune and every other domestic military base, a step that would save taxpayers about \$1 billion a year.

He called several large retailers to see if they would be willing to take over the markets. None were, but Wal-Mart, which has stores within 10 miles of most U.S. bases, proposed offering equivalent discounts to troops, their spouses and their retired brethren. He figured other national chains would follow suit.

When the Defense Department bureaucracy that runs the commissaries learned of Spencer's plan, it sounded an alarm among allies in industry and in Congress. A trade group whose mission is to represent companies that sell goods in military stores fired off a letter to Defense Secretary Robert M. Gates, warning him it would be "ill-advised" to make major changes. Senators and representatives dispatched similar missives. So did veterans groups. As the correspondence stacked up in his inbox, Gates summoned Spencer and other members of the Defense Business Board.

"Richard, my fax machine is vomiting letters of complaint," Spencer recalled Gates telling him. Worried that congressional anger would doom other Pentagon cost-cutting initiatives, Gates told Spencer to drop his commissary plan.

Maybe it is, but there are several things not being discussed.

First, the article points out that the commissary benefit is worth \$4,400 a year to every military family. Most of those families are getting paid pretty low wages for a job that can kill you – \$28,000 for a Corporal or Specialist with 4 years of experience. Is it any

wonder that some in the military are defending this benefit?

Then there's the shock that retired investment banker Richard Spencer (who probably hasn't had to live on \$28,000 a year for a very very long time, if ever) had when he discovered the commissary's books can't be audited.

What little that arrived stunned him. The agency's antiquated financial systems, he learned, are not compliant with the federal government's accounting standards.

That is a problem. But you know what? I'm far, far more concerned that NSA's antiquated financial systems are also not compliant with the federal government's accounting standards (apparently neither are a number of other intelligence community components), and not just because the dollars involved are far larger. I don't have to worry about unaccounted Cheerios on a commissary shelf starting a new war or reading my email via some off the books program that evades Congressional scrutiny because its budget does.

Then there's the assessment that retired investment banker Richard Spencer made that DOD isn't very good at running supermarkets.

Its workforce was bloated compared with other retailers.

[snip]

Spencer also discovered that the agency's annual subsidy did not include other hidden costs. Commissaries don't have to pay rent. Security services, when needed, are provided by military police.

It didn't take Spencer long to come to a basic conclusion: "Running a chain of grocery stores is not a core competency of the Defense Department."

He thought about proposing that a private company be hired to run the stores. But when he called up several large national retailers, including Wal-Mart, Costco and three grocery chains, he got the same response. "We don't want this," he recalled being told. Too many employees, they said, and they would be unable to lure non-military customers onto access-controlled bases.

He's comparing commissaries, of course, with WalMart. Which has been getting a lot of press this year for its difficulties stocking shelves, in part because it has cut staff so thin that there aren't enough people to get all the merchandise onto shelves.

Maybe, when consumers have the leverage to make demands, they prefer shopping in place with better service than WalMart? Maybe that, like better healthcare, is one of the reasons people will risk their life to join the military?

But here's the funniest part of this story. The Administration is, as we speak, making a sustained argument that commissary employees are "sensitive" employees. It argued—really!—that because a commissary Assistant Manager knew how much Gatorade and sunglasses commissary customers were buying (potentially reflecting knowledge of upcoming deployments)—he should lose all Merit Board protection as a sensitive employee.

Now I, of course, thinks that's a load of horse dung. Nevertheless, it is the horse dung the Executive is peddling. And so long as it is peddling that horse dung, it seems incumbent upon the Executive to keep this nice perk around.

It may be that the billion we'd save by shutting down commissaries would be a net savings once you adjust for the higher wages you'd have to pay lower-ranking service members in exchange. It may be the commissaries are hopelessly

unwieldy.

But I'm very skeptical that this perk – and not the much bigger ticket waste – is the first thing that should be cut to save money.

---

## WHAT IF CHINA NOT JUST HACKED — BUT SABOTAGED — THE F-35?

**Chinese cyberspies have hacked most Washington institutions, experts say**

Over the last week, two perennial stories have again dominated the news. China continues to be able to hack us – including top DC power players – at will. And the F-35 has suffered another setback, this time a crack in an engine turbine blade (something which reportedly happened once before, in 2007).

The coincidence of these two events has got me thinking (and mind you, I'm just wondering out loud here): what if China did more than just steal data on the F-35 when it hacked various contractors, and instead sabotaged the program, inserting engineering flaws into the plane in the same way we inserted flaws in Iran's centrifuge development via StuxNet?

We know China has hacked the F-35 program persistently. In 2008, an IG report revealed that BAE and some of the other then 1,200 (now 1,300) contractors involved weren't meeting security requirements; last year an anonymous BAE guy admitted that the Chinese had been camped on their networks stealing data for 18 months. In April 2009, WSJ provided a more detailed report on breaches going back to 2007.

The Joint Strike Fighter, also known as the F-35 Lightning II, is the costliest and most technically challenging weapons program the Pentagon has ever attempted. The plane, led by Lockheed Martin Corp., relies on 7.5 million lines of computer code, which the Government Accountability Office said is more than triple the amount used in the current top Air Force fighter.

Six current and former officials familiar with the matter confirmed that the fighter program had been repeatedly broken into.

[snip]

Foreign allies are helping develop the aircraft, which opens up other avenues of attack for spies online. At least one breach appears to have occurred in Turkey and another country that is a U.S. ally, according to people familiar with the matter.

[snip]

Computer systems involved with the program appear to have been infiltrated at least as far back as 2007, according to people familiar with the matter. Evidence of penetrations continued to be discovered at least into 2008. The intruders appear to have been interested in data about the design of the plane, its performance statistics and its electronic systems, former officials said.

The intruders compromised the system responsible for diagnosing a plane's maintenance problems during flight, according to officials familiar with the matter.

[snip]

The spies inserted technology that

encrypts the data as it's being stolen;  
as a result, investigators can't tell  
exactly what data has been taken.

And we know the data theft has been ongoing. The RSA secure ID hack two years ago, for example, was used to access Lockheed's computers (though at least in that case Lockheed discovered the breach within two weeks).

Incidentally, Pratt & Whitney – which makes the engines that are experiencing this latest problem – got a \$75 million wrist slap last year for violating export controls and dealing engine control module software to China that it then used to build a military attack helicopter, though that conduct dates back to the 2002 to 2006 period.

In any case, we know the Chinese have had a great deal of access to networks involved in the development of the program. The assumption has always been – publicly at least – that China was just stealing data, both to understand how to counter the plane's defenses but also to reverse engineer its own planes.

Yet we also know that China has dealt us hardware – “counterfeit” chips and the like – with backdoors to allow it access. That is, we know China has engaged in sabotage at a more granular level.

So why wouldn't China try to sabotage the F-35 more systematically, especially as the example of StuxNet unfolded?

Admittedly, it may be foolish to attribute to Chinese guile what can easily be explained by American incompetence. Indeed, it's clear mismanagement deserves a great deal of the blame for the plane's budgetary and performance woes.

But this Bloomberg article describes part of the reason why the F-35 would make such a juicy target for China. First, the F-35 is a central part of our industrial policy, providing jobs here and (if it ever gets off the ground)

exports overseas.

It counts 1,300 suppliers in 45 states supporting 133,000 jobs – and more in nine other countries, according to Lockheed.

[snip]

The F-35 will probably become the dominant export fighter for the U.S. aerospace industry, Gordon Adams, who served as the senior White House official for national security and foreign policy budgets under President Bill Clinton, said in a phone interview.

“This is the last U.S. export fighter standing, and that has saved this program,” said Adams, now a foreign-policy professor at American University in Washington. “There is a huge economic element to the F-35.”

Members of Congress are hesitant to make deep cuts to the project in part because it generates work in their states, Wheeler said. The F-35 supports 41,000 jobs in Texas alone, the most of any state, according to Lockheed’s website. The company assembles the fighter in Fort Worth.

And the multinational development of the plane was supposed to cement a new kind of alliance. As members of that partnership begin to get cold feet, it may affect our larger relationship with those countries.

Overseas, the Pentagon’s partners are balancing concerns about the F-35’s cost with the amount of work sent to their companies.

Allies have agreed to purchase 721 fighters, yet the soaring price is painful for nations with shrinking defense budgets. The estimated cost of



each plane has about doubled to \$137 million since 2001, according to a GAO report last year.

[snip]

Canada had dropped to 65 planes from 80. In December, it said it was reconsidering its commitment to purchase any of the jets after a consultant said the price to buy and maintain them might reach about \$45 billion.

The F-35 program isn't so easy to exit, though. A Lockheed spokesman raised the possibility that Canada would lose its F-35-related business – and jobs – if it didn't buy planes.

[snip]

The partners' commitments should make the U.S. wary of making deep cuts to the F-35 program, said Dov Zakheim, a former defense comptroller who served under President George W. Bush.

"This program was advertised as a major collaborative program with a lot of allies," Zakheim said in a phone interview. "It was sold to our allies as such. What do we do now – pull the rug out from under them at the same time we're complaining they aren't spending enough on defense?"

This latest problem comes just as the those managing the F-35 program prepare to go to Australia to try to convince them to buy these planes rather than more existing Boeings.

Then there's just the sheer magnitude of this program. The program is expected to account for 38% of the Pentagon's procurement needs for 2011 programs. Its cost – \$395.7 billion – already rivals a significant war, and actually running the program may cost a trillion and a half. This is where an unbelievable amount of our time and financial resources are being

directed, and anything China could do to raise those costs, or perhaps even convince us to give up on the sunk costs, I'm sure, would bring it huge strategic benefits. It's like half an Iraq War without the potentially dangerous disruptions in the Middle East, all wrapped up in a bow.

At this point, it's not clear that the plane itself will ever represent a critical threat to China (though Japan has been one of the partners that has sustained its enthusiasm for the plane). The program is more interesting at this point for the way it causes us to blindly continue to pursue the catastrophic imperative that is our Military Industrial Complex. Which would make it the perfect opportunity for China, by sabotaging the program, to magnify and exacerbate our own stupidity.

I'd like to think such sabotage would be impossible to get past the quality control folks at Lockheed, but everything about this program suggests it might not be. The multinational development and the concurrent development schedule (a kind of testing as you go) would make it more likely such sabotage might be missed as well.

I don't know that we would ever know if this clusterfuck was caused with the assistance of China. It's not like Lockheed would publicize such information, just as it asked for another \$100 billion. And I don't want to underestimate the defense industry's ability to screw up all by themselves.

All that said, Chinese sabotage would help to explain part of why this program has been such a colossal clusterfuck.

---

# DOJ GIVES BLACKWATER A WHITEWASH ON FELONY CHARGES



Something funny happened in the Eastern District of North Carolina today. Out of the blue in an extremely significant case, and without particular notice to

interested observers, much less the public, the criminal case against former Blackwater executives for weapons trafficking, and a myriad of other weapons violations, ended. Poof! Gone with an undeserved and inexplicable sweetheart misdemeanor plea.

From local Raleigh outlet WRAL:

A federal weapons case against the defense contractor formerly known as Blackwater Worldwide ended Thursday with misdemeanor pleas by two former executives, who were fined and placed on probation.

The case stems in part from a raid conducted by federal agents at the company's Moyock headquarters in 2008 that seized 22 weapons, including 17 AK-47s. An indictment alleged that the company used the Camden County Sheriff's Office to pose as the purchaser of dozens of automatic weapons.

The indictment also alleged that Blackwater purchased 227 short barrels and installed them on long rifles without registering them and that company officials presented the king of

Jordan with five guns as gifts in hopes of landing a lucrative overseas contract and then falsified federal documents once they realized they were unable to account for the weapons.

Gary Jackson and William Matthews, the former president and executive vice president of the company and both Navy Seals, pleaded guilty Thursday to one count each of failure to keep records on firearms. They were sentenced to four months of house arrest, three years on probation and fined \$5,000.

The original indictment was fifteen counts, count em 15 counts, most all serious felonies with significant punishment in the offing. Now granted, a few counts were pared off after a motion to dismiss by a court order dated February 4, 2013, but significant and substantive counts remained viable against Blackwater executives Jackson and Matthews.

But, instead of taking them to trial, or even extracting a reasonable plea that did justice for the public, the DOJ collaborated with the defense and walked into court without notice today, filed a new information containing a single misdemeanor charge and proceeded to sentence them on the spot to a hand slap.

Here is how the official DOJ Press Release described it:

United States Attorney Thomas G. Walker announced that in federal court today GARY JACKSON and WILLIAM WHEELER MATTHEWS, JR. pled guilty before United States District Judge Louise W. Flanagan, to one count each of failing to make and maintain records related to firearms in violation of Title 18, United States Code, Sections 922(m) and 923(g)(1)(A).

Additionally, Judge Flanagan sentenced JACKSON and MATTHEWS to 3 years

probation, 4 months house arrest with stipulations, and fined them \$5,000.00.

According to the Criminal Information **filed on February 14, 2013**, JACKSON and MATTHEWS, between 2005 and 2007, were employees of a corporate entity formerly known as Blackwater which was a licensed federal firearms manufacturer and dealer, and whose responsibilities for a certain period of time included direct or indirect supervisory authority over employees whose duties included the making and maintenance of records required by federal law. (Emphasis added)

Oh yeah, there was one other mention of note in the release:

The corporate entity formerly known as Blackwater has entered into a Deferred Prosecution Agreement with the government in which it has agreed to extensive ongoing compliance programs and the payment of approximately 7 million dollars in fines.

How nice. The Deferred Prosecution Agreement was actually entered into and noticed back in August of last year. It was easy to see the DPA coming, and as much as the US Government relies on Blackwater/Xe/Academi for their security adventures, it was predictable they would be given a DPA (and, hey, DPAs provide lucrative paydays to former DOJ friends who get set up in cushy monitor jobs).

The DPA was easy to see coming, today's sweetheart plea was not. No, it happened basically as a covert op on the public and interested legal community. Did you notice the bolded date in the DOJ press release? DOJ states the plea was entered on February 14, 2013. What is interesting is that it was not placed on the official court docket until today – at the same

time Judge Louise Flanagan, a conservative Bush appointee, was accepting the plea and sentencing Jackson and Matthews, thus ending the case. All designed so the public would not know and could not have any input. Diametrically contrary to the fundamental precepts of the American justice system.

How little of a wrist slap is the sentence? I've had common DWI clients sentenced to more. Compare and contrast to the punishment the DOJ sought to impose on Aaron Swartz.

The sentence is now done and entered, but what about the process? It was a stunning affront to justice and the public right to know. I have complained relentlessly about the collusion between the DOJ and another Bush era criminal, former Office of Special counsel Chief Scott Bloch. But at least in Bloch there was minimal notice given to the public and we knew what was coming, in spite of inexplicable collusion between the DOJ and the criminal defendant. Not so in the case of these Blackwater executives, Jackson, Matthews, et al.

Even in Bloch, in spite of complete collusion on the part of the DOJ, the court set sentencing for nearly three months after the entry of the plea. Not so with Judge Flanagan and the Blackwater boys. How unusual is it that a Federal court sentences criminal defendants immediately in high profile important cases with important implications like this? VERY UNUSUAL.

In fact it is simply stunning, all the more so considering that the parties and the court hid the fact the plea was entered from the public and the court docket system in the period between the entrance of plea on February 14 and the plea acceptance and immediate sentencing today.

To give you an idea of how out of the ordinary such a sentencing on the spot is, there are directly applicable provisions in the Federal Rules of Criminal Procedure that must be specifically obviated on the record to even

attempt it. Rule 32(c) provides:

**(c) Presentence Investigation.**

**(1) Required Investigation.**

(A) In General. The probation officer must conduct a presentence investigation and submit a report to the court before it imposes sentence unless:

(i) 18 U.S.C. §3593 (c) or another statute requires otherwise; or

(ii) the court finds that the information in the record enables it to meaningfully exercise its sentencing authority under 18 U.S.C. §3553, and the court explains its finding on the record.

(B) Restitution. If the law permits restitution, the probation officer must conduct an investigation and submit a report that contains sufficient information for the court to order restitution.

18 USC 3593 concerns death penalty cases, so the ONLY way Jackson and Matthews could have been sentenced today is for the court to have made a specific finding, based upon information on and in the record, and then stated the specific reasons for the decision, and evidence supporting it, *all on the record*.

Did Judge Flanagan do that? Well, we do not know because there is no sentencing minute entry on the docket as there normally is. It just isn't there. What's more, we cannot know if there was a stipulation to hide the plea entry and immediate sentencing plans in the plea agreement (docket number 364), because the plea agreement is SEALED.

All ability of the public to know this was coming, and to discern what really happened, has been secreted from the public. Secret justice (or, more properly, injustice).

How and why did all this occur? Undoubtedly because of the highly classified and incestuous relationship between Blackwater and the US Government, and the resulting ability of Blackwater to literally blackmail and extort concessions through graymail threats (See here for a short history of graymail).

So, through secrecy, classification, graymail and direct collusion with the DOJ, Blackwater, and its executive henchmen, win and the American public lose yet again. I have been practicing criminal law for 25 years and I am absolutely offended by what occurred in Judge Louise Flanagan's courtroom today. Both she and the Obama Department of Justice should be made to answer for it.

[UPDATE: It appears the plea agreement itself is not completely sealed, it is just kept "unavailable" from the public docket. Upon information and belief, it can be viewed if you personally go to the clerk's office for the Eastern District of North Carolina and ask to see it. The other items described in the post as missing from the docket entirely remain so missing.]

---

## **MR. MORAL RECTITUDE'S SLEAZY PAYMENT**

According to Defense News, John Brennan was paid roughly \$2,090 a day while working for The Analysis Corporation in 2008. He was paid roughly \$8,496 for each of the 20 days he worked in 2009 before he became Obama's counterterrorism czar.

A review of Brennan's financial disclosure reports indicates that in 2009, TAC paid him a total of \$169,923



in salary and bonus, which has not been previously reported. The financial disclosure reports, submitted as required of all White House employees, don't say why he'd receive a bonus if he was leaving the company to join the government, or why he'd received such a large salary if he worked for the company for only 20 days that year.

In November 2008, two months before Brennan joined the Obama administration, TAC announced that the CEO was taking a "leave of absence" from the firm. That is, it is not clear that he was actually on the clock for the transition period before he received that \$169,000.

Mind you, this isn't anything that such illustrious people as Dick Cheney haven't already done (and in larger figures, too).

Tim Shorrock provided some background on the company in his book.

There were questions about Brennan's ties to his former company when it was part of the investigation into the failure to connect-the-dots before the UndieBomber attempted to strike the US, though as part of an ethics waver he agreed to recuse himself from anything specifically pertaining to TAC.

The White House has granted a special ethics waiver to allow President Obama's top counterterrorism adviser to conduct a review of the intelligence and screening breakdown that preceded the failed Christmas Day bombing attempt on an American passenger plane over Detroit.

[snip]

Mr. Brennan, who was a longtime C.I.A. officer, needed the waiver because for more than three years before his current post he was chief

executive of the Analysis Corporation, an intelligence firm that provides services to the government. Norm Eisen, the White House ethics counsel, wrote on the White House Web site on Wednesday that Mr. Brennan's past ties to the company, were outweighed by his knowledge of the nation's intelligence system.

And, of course, Brennan's the guy who has sacrificed US privacy to get more data in databases.

The umbrella company that has absorbed TAC continues to get lots of contracts doing intelligence analysis.

---

## TOM COBURN TAKES ON THE ZOMBIE APOCALYPSE



I tell you, if Tom Coburn just stuck to shutting down the most egregious Homeland Security fearmongering boondoggle abuses rather than shutting down government itself, I might grow to love

the man.

His latest effort (for which some of his staffers appear to have staged a very fun photo

shoot) takes on the stupid things localities bought under the \$7.1 billion Urban Area Security Initiative, which was originally intended to help likely terrorist targets (like NYC) prepare against an attack, but which turned into a big boondoggle for towns unlikely to be targeted.

The describes how Keene, NH (home of the Free State Project) tried to use a grant to buy its 40-cop police department—which has faced just one murder in the last two years—an armored vehicle to protect its annual pumpkin festival. Keene was not alone; the report has several pages dedicated to the graft Lenco Armored Vehicles has been conducting selling governments in Waukesha, WI and Santa Barbara, Carlsbad, Escondido, and Fontana, CA BearCats they have no need for using sole source bids.

The report attacks Pittsburgh for having bought an LRAD—which it used during the G-20—as “a kinder and gentler way to get people to leave.” It also describes how San Diego County used an LRAD to protect a speaking event with Darrell Issa, Duncan Hunter, and Susan Davis.

But the center piece of the report is the description of how



first responders used grant money to attend a training session in a San Diego resort at which they were entertained by a Zombie Apocalypse simulation billed as “a very real exercise, this is not some type of big costume party.”

One notable training-related event that was deemed an allowable expense by DHS was the HALO Counter-Terrorism Summit 2012. Held at the Paradise Point Resort & Spa on an island outside San Diego,

the 5-day summit was deemed an allowable expense by DHS, permitting first responders to use grant funds for the \$1,000 entrance fee. Event organizers described the location for the training event as an island paradise: “the exotic beauty and lush grandeur of this unique island setting that creates a perfect backdrop for the HALO Counter-Terrorism Summit.

[snip]

The marquee event over the summit, however, was its highly-promoted “zombie apocalypse” demonstration. Strategic Operations, a tactical training firm, was hired to put on a “zombie-driven show” designed to simulate a real-life terrorism event.<sup>92</sup> The firm performed two shows on Halloween, which featured 40 actors dressed as zombies getting gunned down by a military tactical unit. Conference attendees were invited to watch the shows as part of their education in emergency response training. Barker explained that, “the idea is to challenge authorities as they respond to extreme medical situations where people become crazed and violent, creating widespread fear and disorder.”<sup>93</sup>

According to the firm’s public relations manager, the exercise was brought about “utilizing Hollywood magic,” and setup in a “parking lot-sized movie set [with] state-of-the-art structures, pyrotechnic battlefield effects, medical special effects, vehicles and blank-firing weapons.”<sup>94</sup> Barker added, however, ““This is a very real exercise, this is not some type of big costume party.”<sup>95</sup>

The report also criticizes the way cities scramble to define themselves as high risk, focusing particularly on Thousand Oaks-Oxnard,

but also calling out his own state's Tulsa for its recent UASI grants.

As per usual, DHS can't justify much of this spending. Of particular interest, however, the report reveals that FEMA refused to give Coburn's staffers data on how cities were defined as risks under the Bush Administration.

A fuller explanation of the reasoning for including 14 new jurisdictions in FY2008 was not given, however, and the risk scores for the FY2004-FY2008 DHS uses to award funds is neither public nor was it made available to staff upon request.<sup>69</sup>

<sup>69</sup> Urban area risk scores were made available for 2009-2011. Despite the request, FEMA did not make the risk scores available for FY 2003-2008.

And the whole report is prefaced by some very sound remarks about security.

The balancing act between liberty and security has been tenuous throughout the history of our nation, founded upon basic freedoms granted by our Creator and protected from government infringement within the Bill of Rights of our Constitution. But a new element has been added to this equation over the past decade that threatens to undermine both our liberty and security— excessive government spending and insurmountable debt.

We cannot secure liberty and guarantee security simply by spending more and more money in the name of security. Every dollar misspent in the name of security weakens our already precarious economic condition, indebts us to foreign nations, and shackles the future of our children and grandchildren.

Yeah, Coburn is being a fiscal miser. But in this case, he's absolutely right: this pork does nothing to keep us safe, it militarizes totally safe cities, and makes a bunch of corrupt contractors rich in the process.

---

## **DID MICHAEL HAYDEN PICK THE CONTRACTOR FOR MITT'S VOTER TURNOUT WEBSITE?**

A lot of people are laughing at this account of Mitt Romney's ORCA—and automated GOTV tracking system. Rather than the efficient new system that would leapfrog Obama's turnout machine, the system crashed even before the evening rush started.

The entire purpose of this project was to digitize the decades-old practice of strike lists. The old way was to sit with your paper and mark off people that have voted and every hour or so, someone from the campaign would come get your list and take it back to local headquarters. Then, they'd begin contacting people that hadn't voted yet and encourage them to head to the polls. It's worked for years.

From the very start there were warning signs. After signing up, you were invited to take part in nightly conference calls. The calls were more of the slick marketing speech type than helpful training sessions. There was a lot of "rah-rahs" and lofty talk about how this would change the ballgame.

Working primarily as a web developer, I had some serious questions. Things like

"Has this been stress tested?", "Is there redundancy in place?" and "What steps have been taken to combat a coordinated DDOS attack or the like?", among others. These types of questions were brushed aside (truth be told, they never took one of my questions). They assured us that the system had been relentlessly tested and would be a tremendous success.

[snip]

Now a note about the technology itself. For starters, this was billed as an "app" when it was actually a mobile-optimized website (or "web app"). For days I saw people on Twitter saying they couldn't find the app on the Android Market or iTunes and couldn't download it. Well, that's because it didn't exist. It was a website. This created a ton of confusion. Not to mention that they didn't even "turn it on" until 6AM in the morning, so people couldn't properly familiarize themselves with how it worked on their personal phone beforehand.

[snip]

From what I understand, the entire system crashed at around 4PM.

FWIW, Obama's campaign had two innovations from 2008 this year. For vote trackers—the same purpose as this website was supposed to serve—they had bar code labels for each voter that the tracker would collect on a sheet to be picked up; I assume—but did not see—someone came and picked up those labels and used them later in the day.

For voting problems, they had a great website that showed the campaign where problems were across the country. That's the website I used. The website worked great. We got advance access to it to practice. And the customer service was

amazing: I had a login problem; I submitted a request to fix it, and it got it fixed 6 minutes after I made the request—I'm hoping OFA buys out Comcast.

There was, for me, one significant problem though: you could only enter problems via the polling place name, not the precinct or the address. I didn't get my assignment until after I went to bed (very early) the night before the election, so I just got up, checked my phone, and drove there; never really processed what the name of my polling location was. Even if I had, it wouldn't have been easy to work with: I was in Reform Christian Church Number Yadda Yadda. Given how common Reform Christian Churches in this part of MI and how generic their names are, its name was the functional equivalent of "McDonalds number 2,364." So for user interface reasons, it didn't work as well for me as planned. (By comparison, when I called in with problems in 2008 and said I was at "the firehouse," the local person on the other end of the line knew precisely where I was.)

All that said, the actual website was very nice, and worked well.

So there's a direct comparison to be made.

Even more, though, this account made me think of one thing: how Mitt Romney advisor Michael Hayden paid SAIC \$1 billion to do what NSA could have done, far better, for \$3 million. As with that program, Mitt apparently paid a lot of money to get a program that didn't perform the function it was supposed to.

That—like Mitt's habit of contracting things out at expensive rates, like his award of big bonuses to the top aides who were deluding him but not the actual workers who would do things like make the voter tracker system work—seems so typical of the GOP way of doing things. Expensive, ineffective overkill.

But hey. The contractors get paid even if the candidate doesn't win!



Update: Politico has more.

It's been reported the system crashed at 4 p.m., but multiple sources familiar with the war room operation said it had actually been crashing throughout the day. Officials mostly got information about votes either from public news sources tracking data, like CNN.com, or by calling the counties for information, the source said. Officials insisted the day after the election that they had still believed they were close, and that they had hit their numbers where they needed to, even as Fox News and other outlets called the race.

The numbers in the interface never moved, leaving officials in Boston and out in the states "flying blind" – a phrase used by several people. The workers on the ground didn't know what doors to knock on or what efforts to make with which voter targets who had not yet turned out – some efforts were made but they were slow and more cumbersome. And the campaign officials also generally didn't know which precincts to send auto-calls into to try to boost turnout – especially in precincts in Ohio, where there is no party affiliation in the general election. Instead of targeted information, all they really had to work with was the generic raw vote tallies in various counties.

"The whole point of this system was we were supposed to be able to identify who in these precincts had not turned out, who were our supporters," said one source of the system, which was built at a "substantial" cost. The idea behind it was to use pre-canned, targeted messages to push the voters who hadn't yet cast a ballot, one of the most basic aspects of Election Day GOTV, which is knowing

which supporters have already voted and who still needs to be part of a pull operation.

FWIW, there were several Republican challengers in my poll over the course of the time I was there. They were in close-and effective-phone conversation with the campaign, presumably at the state level. Of course, they weren't tracking voters at this poll--there were only 40 votes cast for Mitt over the entire day. Mostly, they were looking glumly at the long line of African American voters waiting to legally cast their vote--there was nothing they could do. Still--in a county with a very well run Republican Party, they were well organized, albeit entirely by phone.

---

## **ANOTHER BREACH OF CONTRACTOR- PROTECTED CRITICAL INFRASTRUCTURE**

In my never-ending campaign to document all the ways the private sector is a bigger risk to our critical infrastructure than terrorists, hackers, political activists, or average citizens, take a look at the job Raytheon's \$100 million security system for JFK Airport has done.

Daniel Casillo, 31, was able to swim up to and enter the airport grounds on Friday night, past an intricate system of motion sensors and closed-circuit cameras designed to to safeguard against terrorists, authorities said.

[snip]

"We have called for an expedited review of the incident and a complete investigation to determine how Raytheon's perimeter intrusion detection system-which exceeds federal requirements-could be improved. Our goal is to keep the region's airports safe and secure at all times," the Port Authority said in a statement.

This comes just weeks after an 82 year old peace activist was able to breach the security provided by failed Olympic security contractor G4S. In response to that failure, POGO is calling out Energy Secretary Steven Chu for his history of outsourcing to poorly-overseen contractors.

Energy Secretary Steven Chu said in a statement provided to the Knoxville News Sentinel on Monday: "The department has no tolerance for security breaches at any of our sites, and I am committed to ensure that those responsible will be held accountable." But there is no denying that Y-12 [the actual part of Oak Ridge breached] was a giant failure of federal oversight. Now the people being axed are lower-level employees rather than those who have allowed the security standards to fall far below acceptable levels, such as Secretary Chu, himself.

Secretary Chu should be the first on the chopping block. He has been preaching for years that government overseers should get off the back of the contractors and everything will be fine. Then, of course, he is shocked when Y-12 is successfully attacked by an 82-year-old nun.

After only one year in the position, Secretary Chu's deputy secretary, Daniel B Poneman, sent a memorandum (PDF) to the department with a safety and

security reform plan aimed at curtailing pesky government oversight. “Contractors are provided the flexibility to tailor and implement safety programs in light of their situation without excessive Federal oversight or overly prescriptive Departmental requirements,” the memo said.

It should be clear by now that the current culture at DOE and its semiautonomous National Nuclear Security Administration (NNSA) is to take their orders from contractors and provide little or no oversight. As the previous head of contractor-operated laboratory, Lawrence Berkeley National Laboratory, Secretary Chu made clear his disdain for federal oversight, DOE insiders told the Project ON Government Oversight (POGO). In fact, he’s been successful in creating a culture of federal hands off the contractors in the weapons complex.

Now, maybe it’s the case that it’s just too hard to protect these sites from 82 year old nuns and jet skiers wearing bright yellow life-jackets. Maybe it’s the case that there’s no such thing as perfect security (though you wouldn’t know it from the security theater that we all have to pass through to board a plane).

But it sure seems like private contractors are proving inadequate to the task of securing some of our most obvious security targets.

---

## **BLACKWATER’S SLAP ON THE WRIST FOR GUN**

# SMUGGLING AND ARMS TRAFFICKING

Viewed

from

one

perspe

ctive

the

facts

that

  
ACADEMI LLC on its own behalf and on behalf of its predecessors-  
in-interest, subsidiaries, divisions and affiliates identified  
as ACADEMI.

  
Representative of the Retained Entities identified in  
Attachment

  
LEE H. RUBIN  
Counsel for ACADEMI LLC and former affiliates

Blackwater has admitted to amount to running guns—precisely the crime that Fast and Furious attempted to combat. Viewed from another perspective, Blackwater's actions amount to the same kind of thing Viktor Bout is in prison for: making weapons deals with sanctioned entities.

But Blackwater will suffer no more than a wrist slap for such things: a \$7.5 million fine, a third of which can be credited to implementing a compliance system that is substantially already in place, as well as a \$42 million Consent Agreement fine it signed two years ago. (It has paid two \$6 million installments of the \$42 million fine it owes to State Department; even while it continues to get contracts with State)

That doesn't make the Deferred Prosecution Agreement any less funny.

There are the repeated lists of all the aliases of Blackwater—by my count some 37 companies or subsidiaries. Just in case you needed master list of how many times it has tried to change its identity.

There's the bragging about Blackwater's new compliance structure (paid for, presumably, as part of this fine), featuring John Ashcroft (the monitor on one of the most corrupt DPAs ever) and former AIG (AIG?!?!?!?) compliance whiz Suzanne Folsom.

There's the way it says Blackwater can't charge the government any aspect of its fine (what is left after its credit for compliance

infrastructure, that is). Only in DPAs is money not fungible, I guess.

There's the way they try to guard against Blackwater rebranding again (the DPA is written in the name Academi and invokes Xe) by selling itself to someone else. (There's apparently an Erik Prince declaration I'm going to have to chase down tomorrow.)

And there's the way that of those who signed this DPA for Blackwater, only the name of the attorney is included in the text.

Now maybe I shouldn't be laughing so hard. The DPA implies that the US Attorney in North Carolina's Eastern District, Thomas Walker, is still investigating. Maybe Erik Prince will go to jail? Ha!

But this DPA is more a case study in the myriad ways corporate entities escape all justice in this day and age than any real accountability for the same kind of actions we impose stiff sentences on others for.

As always, the lesson is if you're going to commit crimes, do it as a corporation.

---

## **NUKE SITE BREACHED JUST DAYS AFTER SSCI MOVED TO ELIMINATE REPORTING ON NUKE SITE SECURITY**

I have been dawdling about writing this post, in which I explain that two of the reporting requirements the Senate Intelligence Committee rather stupidly, IMO, moved to eliminate last week pertain to the security of our nuclear labs.

Back when I criticized the plan to eliminate these reports in June, I wrote,

The bill would eliminate two reporting requirements imposed in the wake of the Wen Ho Lee scandal: that the President report on how the government is defending against Chinese spying and that the Secretary of Energy report on the security of the nation's nuclear labs. Just last year, the Oak Ridge National Laboratory had to separate from the Internet because some entity—China would be a good candidate—had hacked the lab and was downloading data from their servers. Now seems a really stupid time to stop reporting on efforts to avoid such breaches.

In spite of these very obvious reasons, the Senate did indeed eliminate two reporting requirements pertaining to national labs (though they kept the one pertaining to Chinese spying).

(7) REPEAL OF REPORTING REQUIREMENT REGARDING COUNTERINTELLIGENCE AND SECURITY PRACTICES AT THE NATIONAL LABORATORIES.—Section 4507 of the Atomic Energy Defense Act (50 U.S.C. 2658) is repealed.

(8) REPEAL OF REPORTING REQUIREMENT REGARDING SECURITY VULNERABILITIES OF NATIONAL LABORATORY COMPUTERS.—Section 4508 of the Atomic Energy Defense Act (50 U.S.C. 2659) is repealed.

I'm glad I waited. Now I can use this story to demonstrate how vulnerable our nuclear labs remain.

The U.S. government's only facility for handling, processing and storing weapons-grade uranium [Oak Ridge National Lab] was temporarily shut this week after anti-nuclear activists, including an 82-year-old nun, breached

security fences, government officials said on Thursday.

[snip]

The activists painted slogans and threw what they said was human blood on the wall of the facility, one of numerous buildings in the facility known by the code name Y-12 that it was given during World War II, officials said.

While moving between the perimeter fences, the activists triggered sensors which alerted security personnel. However, officials conceded that the intruders still were able to reach the building's walls before security personnel got to them.

When James Clapper's office asked to throw these reports out, they justified it by saying they could just brief the information rather than report it regularly.

This reporting requirement should be repealed because it is over a decade old and the Secretary of Energy and the National Counterintelligence Executive can provide the information requested through briefings, as requested, if congressional interest persists.

Oak Ridge Lab has been breached twice in two years, once via its computer systems and now physically. I'm sure Congress will be getting a slew of briefings about the lab, but it really does seem like a little reporting requirement might help DOE to take this seriously.