IN DISMISSING RICIN CHARGE AGAINST WHITE SUPREMACIST, JUDGE THROWS ENFORCEMENT OF BIOTERRORISM LAW INTO CHAOS

As pointed out first by Nick Watson in the Gainesville (Georgia) Times and then fleshed out further by Chris Joyner in the Atlanta Journal-Constitution, US District Judge Richard Story on September 21 dismissed a charge of possession of the deadly poison ricin against William Christopher Gibbs. Gibbs had been identified after his arrest by the Southern Poverty Law Center's Hatewatch as a member of the bizarre Georgia Church of Creativity:

> Gibbs claims membership in the "Georgia Church of Creativity," a white supremacy sect that professes "race is our religion," that the "white race is nature's finest," and that "racial loyalty is the greatest of all honors, and racial treason is the worst of all crimes."

In his indictment, Gibbs was charged by a grand jury:

COUNT ONE

On or about February 2, 2017, in the Northern District of Georgia, the defendant, WILLIAM CHRISTOPHER GIBBS, did knowingly possess a biological agent and toxin, to wit, ricin, where such agent and toxin is a select agent for which the defendant had not obtained a registration required by regulations under section 351A(c) of the Public Health Service Act, in violation of

Title 18, United States Code, Section 175b(c).

A TRUE BILL

FOREPERSON

JOHN A. HORN
United States Attorney

In his order directing that the charge be dismissed, Judge Story frames his decision as being due to a mere "clerical error" by the government in drawing up the underlying law and fleshing out the details in subsequent publication of rules. As Joyner described it:

> A north Georgia white supremacist arrested last year for alleged possession of the deadly toxin ricin is no longer facing federal charges after a judge dismissed the case – on a technicality that exposes a regulatory failure.
>
> In an order signed Sept. 21, U.S. District Court Judge Richard Story agreed with the man's legal team that changes to federal law in 2004 and regulatory edits in 2005 inexplicably excluded ricin from the criminal charge of possession of illegal biological toxins known as "select agents."

The huge problem here is that ricin is not the only agent that now, due to this error, falls outside the list of those proscribed from possession. Congress delegates the development and maintenance of the list of "select agents" to which this law applies to the Department of Health and Human Service for those agents that are human pathogens or toxins and to USDA for those agents that affect livestock or crops. The

law also recognizes that some agents on these two lists will overlap, posing threats both to human and agricultural targets.

As Story details in his order, Congress revised the underlying law in late 2004. The list of select agents at that time showed clearly that ricin fell squarely within the purview of the law. But just a few months later, in early 2005, HHS revised its list and in this process, the entire non-overlapping list of human agents suddenly moved to a differently numbered section as it was published. That section number is not listed in the language in the 2004 revision, and so in ruling that Gibbs did not violate the law in possessing ricin, he is in effect making the entire HHS non-overlapping list exempt from the law. That means that under his interpretation, possessing the worst of the worst of the human pathogens or toxins, including even smallpox, cannot be charged under this law.

Here is the language of 18 US Code§ 175b(c), the section cited by the grand jury in the Gibbs indictment:

> (c)UNREGISTERED FOR POSSESSION.—
> (1)SELECT AGENTS.—
> Whoever knowingly possesses a biological agent or toxin where such agent or toxin is a select agent for which such person has not obtained a registration required by regulations under section 351A(c) of the Public Health Service Act shall be fined under this title, or imprisoned for not more than 5 years, or both.
> (2)CERTAIN OTHER BIOLOGICAL AGENTS AND TOXINS.—
> Whoever knowingly possesses a biological agent or toxin where such agent or toxin is a biological agent or toxin listed pursuant to section 212(a)(1) of the Agricultural Bioterrorism Protection Act of 2002 for which such person has not obtained a registration required by regulations under section 212(c) of such Act shall be fined under this title, or

> imprisoned for not more than 5 years, or both.

This part of the law was from the 2004 revision we discussed earlier. In his decision, Story notes that the reading of the whole of 18 US Code§ 175b directs us to the first part of it to find where the list of select agents can be found. It reads:

> *(a)*
> *(1)*
> *No restricted person shall ship or transport in or affecting interstate or foreign commerce, or possess in or affecting interstate or foreign commerce, any biological agent or toxin, or receive any biological agent or toxin that has been shipped or transported in interstate or foreign commerce, if the biological agent or toxin is listed as a non-overlap or overlap select biological agent or toxin in sections 73.4 and 73.5 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act, and is not excluded under sections 73.4 and 73.5 or exempted under section 73.6 of title 42, Code of Federal Regulations.*

> *(2)*
> *Whoever knowingly violates this section shall be fined as provided in this title, imprisoned not more than 10 years, or both, but the prohibition contained in this section shall not apply with respect to any duly authorized United States governmental activity.*

The problem is when we move to the current version of these lists, found here, the numbering for the sections is off when we look at the lists, we see that the entire HHS non-overlapping list is found in section 73.3 and not in 73.4 or 73.5. The agents found in 73.3 are the worst of the worst of agents feared as biological weapons. Even smallpox is on that part of the list, and so, by Story's ruling, now excluded from prosecution.
In his order, Story relies on this garbled numbering to dismiss the charge:

> *As described above, § 175b defines "select agent," as a "biological agent or toxin" that is listed in 42 C.F.R. § 73.4 or § 73.5. This language is unambiguous. And in defining "select agent," the statute does not reference a non-exhaustive list or provide examples; rather, it*

> *says what the term "means." 42 U.S.C. § 175b(d)(l) (emphasis added). '"[M]eans' denotes an exhaustive defmition[.]" StansellL 704 F.3d at 915 filth Cir. 2013) (citing United States v. Probel. 214 F.3d 1285, 1288-89 (11th Cir.2000)). Thus, "[w]hen a statutory definition declares what a term 'means' rather than 'includes/ any meaning not stated is excluded." Id, (citing Colautti v. Franklin, 439 U.S. 379, 392-93 & n. 10 (1979)). Here, neither 42 C.F.R. § 73.4 nor § 73.5 include ricin. The statute does not reference- and thereby excludes-any other sections of the C.F.R. So, applying the statutory definition, as the Court is bound to do, the unavoidable conclusion is that "select agent" under 18 U.S.C. § 175b does not include ricin.2*

Story even knows how the garbled numbering came about:

> *In 2004, as part of the Intelligence Reform and Terrorism Prevention Act, Congress changed the reference from "Appendix A of*

> *part 72" to Part 73. Pub. L. 108-458, 118 Stat. 3638, § 6802(d). This had the effect of criminalizing the possession of "a non-overlap or overlap select biological agent or toxin in sections 73.4 and 73.5 of Title 42" of the C.F.R. However, three months later, HHS re-formatted its regulations, which, in relevant part, resulted in its list of select agents and toxins-including ricin-being moved to a section of the C.F.R. (§ 73.3) that is not referenced in 18 U.S.C. § 175b.*

Story's ruling is technically correct and is a defense attorney's dream. But his justification of it is infuriating:

> *After HHS overhauled its regulatory numbering scheme, Congress had ample opportunity to amend the statute to make its definition of "select agent" comport to the Government's interpretation. It has been 14 years, and Congress is yet to do so. And there are plausible explanations why. For*

> *instance, Congress may have decided that the unregistered possession of ricin, alone, is not conduct sufficiently culpable to justify the commission of a federal crime. Or, Congress may have assumed that the illegality of having certain biological agents and toxins, like ricin, for nefarious purposes is sufficiently encapsulated in other statutory provisions. See 18 U.S.C. § 175. The Court cannot say, but it is not for the Court to disregard a clear statutory definition in favor of absent language that may or may not have been excluded purposefully.*

We are not talking here about a single agent, ricin, being left off the list due to a clerical error. The renumbering left the entire HHS non-overlapping list of agents out of the referenced sections. How on earth could Story believe that Congress would suddenly decide, in early 2005, that the entire HHS non-overlapping list was no longer of concern? Granted, anthrax is on the overlap list and so is still covered under Story's interpretation, but it should be

pointed out that the Amerithrax investigation of the 2001 anthrax attacks was in full gear in 2005 in its march toward hounding Bruce Ivins to his death, so bioterror was a very high priority for Congress and law enforcement at the time of this reclassification. In fact, the boondoggle BioWatch program was launched in 2003 and so in 2005, the generalized fear of bioweapons was pervasive. Also, don't forget the role of bioweapons in general in the Bush Administration run-up to the invasion of Iraq in 2003, complete with Colin Powell's fake vial of anthrax.

Further evidence of the government's intent on the select agent list can be found when one looks for the list itself. For example, this listing clearly shows the government had no intent to exclude the HHS non-overlapping agents and cites relevant statutory authority.

Story attempts, in part, to wriggle out of the deep hole into which he has dug himself by pointing out other ways that Gibbs could be charged. From a footnote in the order:

> *2 The Court notes, however, that the possession of ricin is not a wholly legal endeavor. To the contrary, 18 U.S.C. § 175(a) provides: Whoever knowingly develops, produces, stockpiles,*

> *transfers, acquires, retains, or possesses any biological agent, toxin, or delivery system for use as a weapon,… or attempts, threatens, or conspires to do the same, shall be fined under this title or imprisoned for life or any term of years, or both. In assessing the constitutionality of this provision under the vagueness doctrine, the Eleventh Circuit held, "The statute provides a person of ordinary intelligence with fair warning that possessing castor beans, while knowing how to extract ricin, a biological toxin, from the beans, and intending to use the ricin as a weapon to kill people, is prohibited." United States v. Crump, 609 F. App'x 621, 622 (11th Cir. 2015) (citing United States v. Lebowitz, 676 F.3 d 1000, 1012 (llth Cir.2012) (per curiam)).*

Interestingly, when I went back to look at one of my posts on James Everett Dutschke, who was charged with possessing ricin in Mississippi in 2013, I see that he was indeed charged under 18 U.S.C. § 175(a).

The damage that Story has done in this ruling may not be limited solely to the HHS non-overlapping agents being left out of the law. Another aspect of the garbled re-numbering of sections is that § 73.5 is referenced as a list of proscribed agents. In reality, the section is headed “Exemptions for HHS select agents and toxins”. I would argue that this is further evidence of a simple error and not legislative intent, because it renders the bill unintelligible. Instead of a list of banned agents, it is a list of those that are exempt from the law due to their use in laboratories for diagnosis or research. Although Story does make passing reference to the differences among those agents that are on the list to be banned, those that are excluded and those that are exempt, I fear that opponents of biological research could latch onto Story’s ruling in an attempt to argue that shipment of these research or diagnostic samples could be prosecuted as bioterrorism. That could have a chilling impact on research to protect us from these very agents.

Congress clearly needs to fix this mess, and fix it quickly. Simple language adjustment in 18 US Code§ 175b(a)(1) could restore the law to applying to the proper lists of agents while excluding or exempting those for which it is appropriate.

JOBY WARRICK RETURNS TO BIOWEAPONS SECURITY THEATER

Last night, Joby Warrick put up a dutifully transcribed article in which the intelligence community is warning us to be very afraid that North Korea suddenly has bioweapons capability. Let’s hope North Korean anthrax capabilities

don’t become the next aluminum tubes.

THE SCOPE OF THE SPECIAL COUNSEL APPOINTMENT IS TOTALLY INADEQUATE

I’m agnostic about the selection of Robert Mueller as Special Counsel on the Trump investigation. But I think the scope of his authorization is totally inadequate.

THE JUST RIGHT FEAR INDUSTRY, IN 18,000 WORDS

Steven Brill thinks we’re not worried enough about bioterrorism and dirty bombs. He makes that argument even while acknowledging that a dirty bomb attack launched in Washington DC would result in just 50 additional cancer deaths. And curiously, his extensive discussion about germ threats (inspired by a Scooter Libby report, no less!) doesn’t mention that the Russian military is currently struggling to contain an anthrax attack launched by a thawing reindeer.

That’s the problem with Brill’s opus: anthrax attacks only matter if they’re launched by Islamic extremist reindeers, not reindeers weaponized by climate change. (And if you were wondering, although he discusses it at length, Brill doesn’t mention that the 2001

anthrax attack, which was done with anthrax derived from a US lab, has never been solved.)

He makes a similar error when he spends 18 paragraphs focusing on what he (or his editors) dub "cyberterrorism" only to focus on OPM as proof the threat exists and includes this paragraph from Jim Comey admitting terrorists don't yet have the capabilities to hurt us our Chinese and Russian adversaries do.

> For his part, the FBI's Comey worries more about a cyberterror onslaught directed at the private sector than one directed at the government. "These savages," he says, "have so far only figured out how to use the internet to proselytize, not to wreak physical damage. What happens when they figure out how to use it to break into a chemical plant, or a blood bank and change the blood types? We know they are trying. And they don't have to come here to do it."

Biothreats and hacking are a threat. But it would be sheer idiocy to approach the problem, at this point, as primarily one of terrorism when climate change and nation-state adversaries clearly present a more urgent threat.

But it's not just Brill who adopts some weird categorization. The article is perhaps most interesting for the really telling things he gets Comey to say, as when he suggests FBI drops investigations when they hear a "wing nut" making bomb threats in a restaurant.

> "Think about it from our perspective," Comey said when I asked about this. "Suppose someone is overheard in a restaurant saying that he wants to blow something up. And someone tells us about it. What should we do? Don't we need to find out if he was serious? Or was he drunk? The way to do that is to have someone engage him in an undercover way,

> not show up with a badge and say, 'What are your thoughts in regard to terrorism?' "
>
> "Plenty of times it's a wing nut or some drunk, and we drop it," he continued.

I actually think the FBI, as an institution, is better than this. But to have the FBI Director suggest his bureau wouldn't follow up if someone making bomb threats was deemed a radical but would if they were deemed a Muslim is really telling.

Which gets to the core of the piece. Over the course of the 18,000+ words, Brill admits — and quotes both President Obama and Comey admitting — that what makes terrorism different from the equally lethal attacks by other mentally unstable or "wing nut" types is the fear such attacks elicit.

> President Obama described the difference to me this way: "If the perpetrator is a young white male, for instance—as in Tucson, Aurora, and Newtown—it's widely seen as yet another tragic example of an angry or disturbed person who decided to lash out against his classmates, co-workers, or community. And even as the nation is shaken and mourns, these kinds of shootings don't typically generate widespread fear. I'd point out that when the shooter or victims are African American, it is often dismissed with a shrug of indifference—as if such violence is somehow endemic to certain communities. In contrast, when the perpetrators are Muslim and seem influenced by terrorist ideologies—as at Fort Hood, the Boston Marathon bombing, San Bernardino, and Orlando—the outrage and fear is much more palpable. And yet, the fact is that Americans are far more likely to be injured or killed by gun violence than a terrorist attack."

> The FBI's Comey agrees. "That the shooter in San Bernardino said he was doing it in the name of isil changed everything," he told me. "It generates anxiety that another shooting incident, where the shooter isn't a terrorist, doesn't. That may be irrational, but it's real."

Nevertheless, all three — even Brill, in a piece where he takes Obama to task for not publicizing his change in dirty bomb response, refers to "deranged people and terrorists" obtaining assault weapons as if they are mutually exclusive categories — seem utterly unaware that part of the solution needs to be to stop capitulating to this fear. Stop treating terrorism as the unique, greatest threat when you know it isn't. Channel the money being spent on providing tanks to local police departments to replacing lead pipes instead (an idea Brill floats but never endorses). Start treating threats to our infrastructure — both physical and digital — including those caused by weaponized reindeer as the threat they are.

And for chrissakes, don't waste 18,000 words on a piece that at once scolds for fearmongering even while perpetuating that fear.

THURSDAY: MOVE

Need something easy on the nerves today, something mellow, and yet something that won't let a listener off too lightly. Guess for today that's John Legend's Tiny Desk Concert.

I promised reindeer tales today, haven't forgotten.

From Anthrax to Zombies

- First outbreak in 75 years

forces evacuation of reindeer herders (The Siberian Times) – The last outbreak in the Siberian tundra was in 1941; news of this outbreak broke across mainstream media this past week, with some outlets referring to it as a "zombie" infection since it came back from dormancy, likely rising from a long-dead human or animal corpse.

- Infected reindeer corpses to be collected and destroyed (The Barent Observer) – A lot of odd details about anthrax and its history pop up as the outbreak evolves. Like the mortality rate for skin anthrax (24%) and the alleged leak of anthrax from a Soviet bio-warfare lab in 1979. Reindeer deaths were blamed initially on unusually warm weather (~30C); the same unusually warm weather may have encouraged the release of long-dormant anthrax from the tundra.
- Siberian outbreak may have started five weeks earlier (The Siberian Times) – Russia's Federal Service for Veterinary and Phytosanitary Surveillance senior official

is angry about the slow response to the first diagnosis; the affected region does not have strong veterinary service, and it took a herder four days' walk across the tundra to inform authorities about an infection due to a lack of communications technology. The situation must be serious as the Health Minister Veronika Skvortsova has now been vaccinated against anthrax. Reports as of yesterday indicate 90 people have been hospitalized, 23 of which have been diagnosed with anthrax, and one child died. The form most appear infected with is intestinal; its mortality rate is a little over 50%. Infection is blamed on anthrax-contaminated meat; shipment of meat from the area is now banned. Russian bio-warfare troops have established a clean camp for the evacuated herder families until the reindeer corpses have been disposed of and inoculations distributed across the area's population.

- Important: keep in mind this Siberian outbreak may be

unusual for its location, but not across the globe. In the last quarter there have been small anthrax outbreaks in Indonesia, Kazakhstan, Kenya, Bangladesh, and Bulgaria. Just search under Google News for “anthrax” stories over the last year.

- Coincidentally, anthrax drug maker filed and received FDA’s ‘orphan status’ (GlobeNewsWire) – There have been so few orders for anthrax prophylaxis vaccine BioThrax that specialty biopharmaceutical company Emergent BioSolutions requested ‘orphan status’ from the FDA, granted to special therapies for rare conditions affecting less than 200,000 persons in the U.S. The status was awarded mid-June.
- Investor sues anthrax drug maker for misleading expectations (Washington Business Journal) – Suit filed against the company and executives claims Emergent BioSolutions mislead investors into thinking the company would sell as many doses of BioThrax to the U.S. government during the next

five years as the preceding five years. On the face of it, investor appears to expect Emergent BioSolutions to predict both actual vaccine demand in advance along with government funding (hello, GOP-led Congress?) and other new competitors in the same marketspace. Seems a bit much to me, like the investor feels entitled to profits without risk. Maybe they'll get lucky and climate change will increase likelihood of anthrax infections – cha-ching.
- Another coincidence: Last Friday marked 8 years since anthrax researcher Bruce Ivin's death (Tulsa World) – And this coming Saturday marks six years since the FBI released its report on the anthrax attacks it blamed on Ivins.

Cybernia

- Facebook let police shut down feed from negotiations resulting in another civilian-death-by-cop (The Mary Sue) –Yeah, we wouldn't want to let the public see the police use deadly force against an African American

mother and her five-year-old child instead of talking and waiting them out of the situation as they do so many white men in armed confrontations. And now police blame Instagram for her death. Since when does using Instagram come with an automatic death warrant?

- Can GPS location signals be spoofed? Yep. (IEEE) – It's possible the U.S. Navy patrol boats caught in Iran's waters may have relied on spoofed GPS; we don't know yet as the "misnavigating" incident is still under investigation. This article does a nice job explaining GPS spoofing, but it leaves us with a mystery. GPS signals are generated in civilian and military formats, the first is unencrypted and the second encrypted. If the "misnavigated" patrol boats captured by Iran in January were sent spoofed GPS location data, does this mean U.S. military encryption was broken? The piece also ask about reliability of GPS given spoofing when it comes to self-driving, self-

navigating cars. Oh hell no.

- Security firm F-Secure releases paper on trojan targeting entities involved in South China Sea dispute (F-Secure) – The Remote Access Trojan (RAT) has been called NanHaiShu, which means South China Sea Rat. The RAT, containing a VBA macro that executes an embedded JScript file, was spread via email messages using industry-specific terms. The targets were deliberately selected for spearfishing as the senders knew the users did not lock down Microsoft Office's default security setting to prevent macro execution. The malware had been in the wild for about two years, but its activity synced with events related to the South China Sea dispute.

Tomorrow's Friday, which means jazz. Guess I'd better start poking around in my files for something good. Catch you later!

IS MATT DEHART BEING

PROSECUTED BECAUSE FBI INVESTIGATED CIA FOR THE ANTHRAX LEAK?

Buzzfeed today revealed a key detail behind in the Matthew DeHart case: the content of the file which DeHart believes explains the government's pursuit of him. In addition to details of CIA's role in drone-targeting and some ag company's role in killing 13,000 people, DeHart claims a document dropped onto his Tor server included details of FBI's investigation into CIA's possible role in the anthrax attack.

> According to Matt, he was sitting at his computer at home in September 2009 when he received an urgent message from a friend. A suspicious unencrypted folder of files had just been uploaded anonymously to the Shell. When Matt opened the folder, he was startled to find documents detailing the CIA's role in assigning strike targets for drones at the 181st.
>
> Matt says he thought of his fellow airmen, some of whom knew about the Shell. "I'm not going to say who I think it was, but there was a lot of dissatisfaction in my unit about cooperating with the CIA," he says. Intelligence analysts with the proper clearance (such as Manning and others) had access to a deep trove of sensitive data on the Secret Internet Protocol Router Network, or SIPRNet, the classified computer network used by both the Defense and State departments.
>
> As Matt read through the file, he says, he discovered even more incendiary material among the 300-odd pages of slides, documents, and handwritten

> notes. One folder contained what appeared to be internal documents from an agrochemical company expressing culpability for more than 13,000 deaths related to genetically modified organisms. There was also what appeared to be internal documents from the FBI, field notes on the bureau's investigation into the worst biological attack in U.S. history: the anthrax-laced letters that killed five Americans and sickened 17 others shortly after Sept. 11.
>
> Though the attacks were officially blamed on a government scientist who committed suicide after he was identified as a suspect, Matt says the documents on the Shell tell a far different story. It had already been revealed that the U.S. Army produced the Ames strain of anthrax — the same strain used in the Amerithrax attacks — at the Dugway Proving Ground in Utah. But the report built the case that the CIA was behind the attacks as part of an operation to fuel public terror and build support for the Iraq War.
>
> Despite his intelligence training, Matt was no expert in government files, but this one, he insists, featured all the hallmarks of a legitimate document: the ponderous length, the bureaucratic nomenclature, the monotonous accumulation of detail. If it wasn't the real thing, Matt thought, it was a remarkably sophisticated hoax. (The FBI declined requests for comment.)
>
> Afraid of the repercussions of having seen the folder of files, Matt panicked, he claims, and deleted it from the server. But he says he kept screenshots of the dozen or so pages of the document that specifically related to the FBI investigation and the agrochemical

> matter, along with chat logs and passwords for the Shell, on two IronKey thumb drives, which he hid inside his gun case for safekeeping.

Is it possible DOJ would really go after DeHart for having seen and retaining part of that FBI file?

For what it's worth, I think Bruce Ivins could not have been the sole culprit and it's unlikely he was the culprit at all. I believe the possibility that a CIA-related entity, especially a contractor or an alumni, had a role in the anthrax attack to be possible. In my opinion, Batelle Labs in Ohio are the most likely source of the anthrax, not least because they're close enough to New Jersey to have launched the attacks, but because — in addition to dismissing potential matches to the actual anthrax through a bunch of smoke (only looking for lone wolves) and mirrors (ignoring four of the potentially responsive samples) — Batelle did have a responsive sample of the anthrax. Though as a recently GAO report made clear, FBI didn't even sample all the labs that had potentially responsive samples, so perhaps one of those labs should be considered a more likely source. Batelle does work for the CIA and just about everyone else, so if Batelle were involved, CIA involvement couldn't be ruled out.

So I think it quite possible that FBI was investigating CIA or someone related to CIA in the attack. It's quite possible, too, that someone might want to leak that information, as it has been clear for years that at least some in FBI were not really all that interested in solving the crime. Even the timing would make sense, coming as it would have in the wake of the FBI's use of the Ivins suicide to stop looking for a culprit and even as the Obama Administration was beginning to hint it wasn't all that interested in reviewing FBI's investigation.

But there's something odd about how this was

allegedly leaked.

According to Buzzfeed, the anthrax investigation came in one unencrypted folder with the ag document and a document on drone targeting the source of which he thinks he knows (it would like have been a former colleague from the ANG).

How would it ever be possible that the same person would have access to all three of those things? While it's possible the ag admission ended up in the government, even a DOJ investigation into such an admission would be in a different place than the FBI anthrax investigation, and both should be inaccessible to the ANG people working on SIPRNet.

That is, this feels like the Laptop of Death, which included all the documents you'd want to argue that Iran had an active and advanced nuclear weapons program, but which almost certainly would never all end up on the same laptop at the same time.

And, given DeHart's belief reported elsewhere this was destined for WikiLeaks, I can't help but remember the Defense Intelligence Agency report which noted that WikiLeaks might be susceptible to disinformation (not to mention the HB Gary plot to discredit WikiLeaks, but that came later).

> This raises the possibility that the Wikileaks.org Web site could be used to post fabricated information; to post misinformation, disinformation, and propaganda; or to conduct perception management and influence operations designed to convey a negative message to those who view or retrieve information from the Web site

That is, given how unlikely it would be to find these juicy subjects all together in one folder, I do wonder whether they're all authentic (though DeHart would presumably be able to assess the authenticity of the drone targeting documents).

And DeHart no longer has the documents in question — Canada hasn't given them back.

> Paul told the agents that his family had evidence to back up their account: court documents, medical records, and affidavits — along with the leaked FBI document Matt had found that exposed an explosive secret. It was all on two encrypted thumb drives, which Matt later pulled off a lanyard around his neck and handed to the guards.
>
> [snip]
>
> If Matt is, in fact, wrongly accused, answers could be on the thumb drives taken by the Canada Border Services Agency, which have yet to be returned to the DeHarts. But without access to the leaked files Matt claims to have seen, there is no way to verify whether he was actually in possession of them, and, if he was, whether they're authentic.

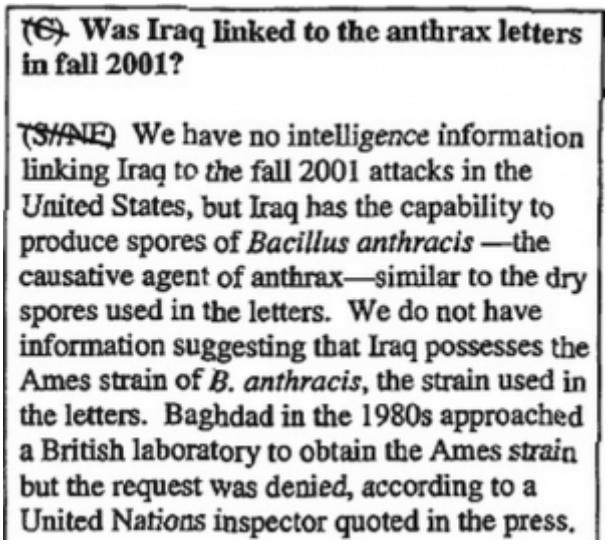
Though at least one person (a friend in London? Any association with WikiLeaks?) may have a copy.

> Inside a hotel room in Monterrey, Mexico, Matt says he copied the Shell files onto a handful of thumb drives. He mailed one to a friend outside London, and several others to locations he refuses to disclose. He also says he sent one to himself in care of his grandmother, which he later retrieved for himself. When the subject of the drives comes up, Matt acts circumspect because, he says, he knows that our communications are being monitored.

There's definitely something funky about this story. Importantly, it's not just DeHart and his family that are acting like something's funky — the government is too.

But that doesn't necessarily mean the FBI thinks CIA did the anthrax attack.

WHAT WAS THE ANTHRAX ATTACK TARGETING PATRICK LEAHY DOING IN THE IRAQ NIE?



~~(C)~~ Was Iraq linked to the anthrax letters in fall 2001?

~~(S//NF)~~ We have no intelligence information linking Iraq to the fall 2001 attacks in the United States, but Iraq has the capability to produce spores of *Bacillus anthracis* —the causative agent of anthrax—similar to the dry spores used in the letters. We do not have information suggesting that Iraq possesses the Ames strain of *B. anthracis*, the strain used in the letters. Baghdad in the 1980s approached a British laboratory to obtain the Ames strain but the request was denied, according to a United Nations inspector quoted in the press.

As Jason Leopold reports, the government recently released a newly declassified version of the 2002 NIE that justified the war with Iraq to Black Vault's John Greenwald. Leopold has a useful overview of what the report includes. But I'm most appalled by this.

> The NIE also restores another previously unknown piece of "intelligence": a suggestion that Iraq was possibly behind the letters laced with anthrax sent to news organizations and senators Tom Daschle and Patrick Leahy a week after the 9/11 attacks. The attacks killed five people and sickened 17 others.
>
> "We have no intelligence information

> linking Iraq to the fall 2001 attacks in the United States, but Iraq has the capability to produce spores of *Bacillus anthracis* — the causative agent of anthrax — similar to the dry spores used in the letters," the NIE said. "The spores found in the Daschle and Leahy letters are highly purified, probably requiring a high level of skill and expertise in working with bacterial spores. Iraqi scientists could have such expertise," although samples of a biological agent Iraq was known to have used as an anthrax simulant "were not as pure as the anthrax spores in the letters."

Perhaps the inset discussing the US-developed anthrax used to attack two Senators and members of the media purports to respond to questions raised by anonymous sources leaking the previous year. But it basically does nothing but suggest the possibility Iraq might have launched the attack, even while providing one after another piece of evidence showing why that was all but impossible.

Moreover, by the time this NIE was completed in October 2002, that deliberate leak had been silent for a almost a year.

That the rumor appeared again, secretly, in the Iraq NIE really ought to raise questions about a whole slew of unanswered questions about the anthrax attack: about why Judy Miller got fake anthrax, about why the FBI scoped its investigation to find only lone wolves and therefore not to find any conspirators (and still almost certainly hasn't found the culprit), about why the first person framed for the attack also happened to be someone who knew of efforts to reverse engineer Iraq's purported bioweapon labs.

No. No, Iraq wasn't linked to the anthrax letters in fall 2001. It's a simple answer. But nevertheless, the question got treated as a

serious possibility when Bush Administration was trying to drum up war against Iraq.

AS FBI'S AMERITHRAX CASE CONTINUES TO CRUMBLE, BUREAU DIGS IN ON NORTH KOREA CLAIMS

Less than 10 days ago, Jim laid out yet more evidence that the FBI's claimed explanation for the anthrax attack — that USAMRIID researcher Bruce Ivins not only perpetrated the attack, but did so acting alone — was scientifically problematic. So 13 years ago, anonymous sources blamed Iraq for the attack, 12 years ago they blamed Steven Hatfill, and 6 years ago, they started blaming Bruce Ivins. Probably, none of those claims are true.

The FBI still hasn't solved one of the most alarming terrorist attacks in this country, an attempt to kill two sitting US Senators. Instead, it persists in a claim (versus Ivins) that doesn't comport with the science, to say nothing of the other circumstantial evidence. FBI only ever sustained that claim by assuming — based on no known evidence — that a Lone Wolf, rather than conspirators, launched the attack.

Even as new evidence undermining the FBI's obstinate claims about Ivins got released, the FBI has been making equally obstinate claims that North Korea is behind the Sony hack.

And then someone crashed North Korea's Internet which, given how tiny it is, is the strategic equivalent of launching spitballs at a small group of North Korea's elite. A truly awesome use of American power!

As I noted on Salon, even as the FBI was leaking its certitude to the big press that North Korea was behind the hack, Kim Zetter was pointing out all the reasons that made no sense.

Now, with a week of holiday cheers under their belts, more of the press is beginning to note all the experts questioning the FBI's claim. Shane Harris describes the FBI "doubling down" on its original theory.

> In spite of mounting evidence that the North Korean regime may not have been wholly responsible for a brazen cyberassault against Sony—and possibly wasn't involved at all—the FBI is doubling down on its theory that the Hermit Kingdom solely bears the blame.
>
> "We think it's them," referring to the North Koreans, an FBI spokesperson told The Daily Beast when asked to respond to reports from private investigators that other culprits were responsible. The latest evidence, from the cyberanalysis firm the Norse Corp., suggests that a group of six individuals, including at least one disgruntled ex-Sony employee, is behind the assault, which has humiliated Sony executives, led to threats of terrorist attacks over the release of a satirical film, and prompted an official response from the White House.
>
> The FBI said in a separate statement to journalists on Monday that "there is no credible information to indicate that any other individual is responsible for this cyberincident." When asked whether that left open the possibility that other individuals may have assisted North Korea or were involved in the assault on Sony, but not ultimately responsible for the damage that was done, the FBI spokesperson replied, "We're not making the distinction that you're making about the responsible

> party and others being involved."

Time catalogs the alternatives to FBI's theories.

And Politico notes that when one cybersecurity company, Norse, shared its analysis, the FBI refused to share its own data, as the company had expected.

> The FBI says it is standing by its conclusions, but the security community says the agency has been open and receptive to help from the private sector throughout the Sony investigation.
>
> Norse, one of the world's leading cyber intelligence firms, has been researching the hack since it was made public just before Thanksgiving.
>
> Norse's senior vice president of market development said the quickness of the FBI's conclusion that North Korea was responsible was a red flag.
>
> "When the FBI made the announcement so soon after the initial hack was unveiled, everyone in the [cyber] intelligence community kind of raised their eyebrows at it, because it's really hard to pin this on anyone within days of the attack," Kurt Stammberger said in an interview as his company briefed FBI investigators Monday afternoon.
>
> He said the briefing was set up after his company approached the agency with its findings.
>
> Stammberger said after the meeting the FBI was "very open and grateful for our data and assistance" but didn't share any of its data with Norse, although that was what the company expected.

It's a bad thing, given how much evidence is out there about this hack, that the FBI won't let more of its thinking be tested publicly.

Meanwhile, in a remarkable joining of opinion, both Jack Goldsmith and Moon of Alabama note that Obama may have wasted US credibility by so quickly accusing North Korea.

And NYT's Ombud, Margaret Sullivan, admits that NYT too quickly repeated — and granted anonymity to — FBI's flimsy claims.

> [A]s a reader, Brad Johnson, noted in an email. He wrote: "Did NYT learn its lesson from the Iraq WMD debacle, or is the paper back to bad habits of writing stories from whole cloth based on anonymous White House and intelligence agency officials?"
>
> Now that the matter of who was behind the hack is coming under more scrutiny, including in The Times (though with less prominence), those kinds of questions are even more germane.
>
> One thing is certain: Anonymity continues to be granted to sources far more often than a last-resort basis would suggest.

Though Sullivan's caution didn't lead the Editorial Board to show any.

I'm glad people are now showing skepticism, even if it is too late to preserve American credibility (as if we had that anyway after StuxNet).

There's one more factor that deserves notice here: the role of cybersecurity firms in laundering government propaganda.

One of the most pregnant observations in Zetter's *Countdown to Zero Day* comes after Symantec published the first details implicating the US and Israel in the StuxNet attack. The Symantec team expected a bunch of

others to jump in and start validating their work. Instead, they were met with almost complete silence. While Zetter didn't say it explicitly, the implication was that the security industry is driven by its interest in retaining the good will of the US Government. Here, the first security firm to back the North Korea claim was Mandiant, the firm that served as a surrogate for claims against China.

And while in this case there is no lack of experts willing to push back against US claims, I just wonder whether at least some of the initial credulity on the North Korea claims arose because of the dominance of USG contractors among the earliest reports on the hack? While there are some equivalents in the WMD vein, the cyberindustry, in particular, seems particularly prone to serving as a cut-out for both poorly analyzed intelligence and even propaganda.

Ah well. It's not like anyone is demanding FBI resume its hunt for the terrorist who might have killed two sitting US Senators. Why do I think this will be any different?

GAO ANALYSIS HIGHLIGHTS LAB SAMPLES EXCLUDED IN SLOPPY FBI ANTHRAX INVESTIGATION

As the last Friday before Christmas, late yesterday afternoon was the most obvious Friday news dump hour of the year, and the government didn't disappoint. The Government Accountability Office released the results of a twenty-three month long study of the genetic analysis that

was used to tie the material found in the anthrax attacks of 2001 to the laboratory of Bruce Ivins, whom the FBI concluded (pdf) was solely responsible for the attacks. The FBI's conclusion is highly suspect for many reasons. On the science side, it is very unlikely that Ivins could have produced all of the attack material on his own and the detailed chemistry of the attack spores suggests that highly sophisticated materials and techniques unavailable to Ivins likely were used to prepare the attack material. Regarding that second point, note that even William Broad refers indirectly to the chemistry concerns in his New York Times article on the GAO report:

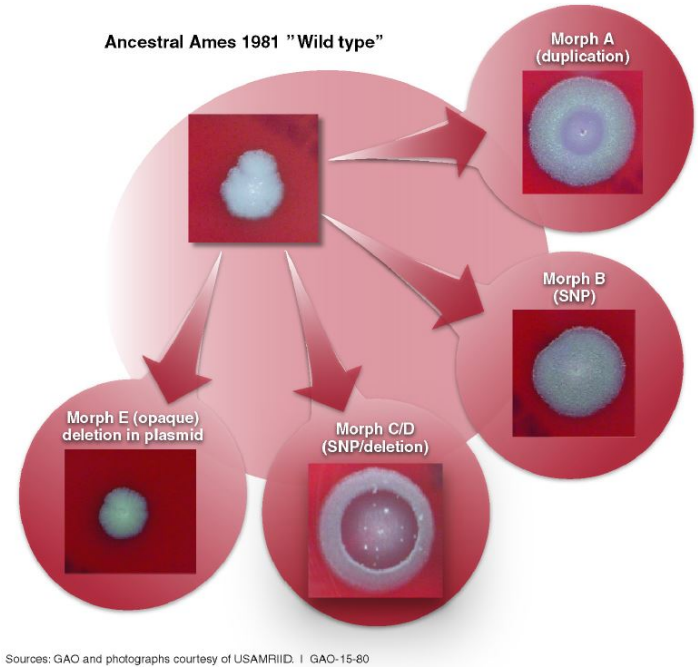
> To the regret of independent scientists, the report made no mention of an issue beyond genetics: whether the spores displayed signs of advanced manufacturing. They have pointed to distinctive chemicals found in the dried anthrax spores that they say contradict F.B.I. claims that the germs were unsophisticated.
>
> Evidence of special coatings, they say, suggests that Dr. Ivins had help in obtaining his germ weapons or was innocent.

The GAO study was undertaken, in part, because of questions raised by the National Academies study released in 2011 and with special prompting by Representative Rush Holt, from whose district the letters likely were mailed. The GAO study focused on obtaining a better understanding of the validity of the genetic analysis that was carried out and the statistics underlying the conclusions reached.

For a refresher, a helpful illustration from the GAO report shows the underlying biology of the genetic analysis that was carried out in the Amerithrax investigation. Here we see photos of a typical colony of the Ames strain of *Bacilus anthracis* on an agar plate and four variant

colony types that occurred at low frequency when the attack material was spread out on agar so that colonies arose from single cells of the overall population of bacteria that were present in the attack material:

Figure 2: Ancestral Ames Strain and Types of Morphs Found in the Evidence from the 2001 Anthrax Attack



DNA sequence analysis was employed to identify the changes that led to these variant colony shapes. The FBI then commissioned private laboratories to develop DNA-based tests (relying on polymerase chain reaction, or PCR, methodology) that could be used to screen the large bank of isolates of the Ames strain that the FBI had accumulated through a subpoena submitted to all 20 laboratories known to have isolates of the Ames strain. Developing these assays represented a new frontier in forensic genetics and it did not prove possible to develop tests for all of the mutations identified in the original DNA sequencing. In the end, four tests were developed by the four different contractors.

The Amerithrax report stated that of the 947 samples included in the final analysis, only eight showed all four of the DNA changes the tests were designed to detect. Seven of those samples came from the laboratory where Ivins worked (U.S. Army Medical Research Institute of

Infectious Diseases, or USAMRIID) and one came from Batelle Memorial Institute in Columbus, Ohio. The FBI noted that there was a record of material being transferred from USAMRIID to Battelle, accounting for the sample found there.

The GAO analysis finds a number of significant issues with the FBI's work:

Source of Variant Types

First, the GAO report noted that during the development of the genetic tests, questions arose about the factors underlying the presence of variants and especially whether culture conditions might affect the relative populations of normal and variant types:

> Although the specific genetic mutations used as genetic markers to determine a match or exclusion were adequately characterized, the FBI did not conduct studies to understand the methods and environmental conditions that gave rise to the mutations. The FBI convened a team of scientists in 2007 to review the scientific methods. Finding no shortfalls or deficiencies in the basic methodologies they reviewed, they determined that the usefulness of the genetic markers was sufficient. The team also stated that the extent of research and development of the genetic tests at the date of their review was insufficient to determine whether the presence or absence of one or several of the genetic markers was associated with the evidence, was merely characteristic of normal culture practices, or possibly was affected by the sensitivity of detections of the genetic tests. The team recommended additional studies to characterize the genetic markers as a function of growth conditions, including the influence of growth time, growth media, and temperature.

The GAO reports that the FBI's response to these concerns when they were raised by the NAS panel was hardly encouraging:

> In response to questions from the NAS panel about this recommendation, the FBI stated that it considered such studies academic and did not conduct the recommended research.

But that is hardly a just an "academic" question. See this post of mine for a summary of the preparation of Ivins' RMR-1029 flask, which the FBI treated as essentially a smoking gun. That flask had material from a large number of large scale cultures. Also, the sheer amount of very highly concentrated material in the recovered letters from the attack also suggest very large cultures were carried out to produce the attack material. By comparison, the material submitted by the laboratories in response to the subpoena would be from very small laboratory scale cultures, and so the growth conditions would have been quite different, quite likely affecting the ratios of variant types in the final populations produced.

Sample Submission

Besides the concerns about culture conditions affecting the presence of variants in the samples submitted, the NAS report highlighted a point that had been somewhat obscured previously. It turns out that the scientists responding to the subpoena showed huge variations in how they responded and what they considered to be separate laboratory populations worthy of sample submission:

> Our analysis of FBI documents shows that FBI searches at three specific laboratories identified hundreds of additional relevant stocks that laboratories did not submit to the repository in response to the subpoena. Specifically, we found that the FBI collected about 29 percent of the 1,059

> repository samples through these searches.

That’s staggering. Nearly a third of the total repository of samples would not have been present had the FBI not searched those three labs. From the Amerithrax report, we do learn that the three that were searched were USAMRIID, Dugway and Batelle. But what about the 17 sites submitting samples that weren’t searched? How many populations were missed in the pool that was tested? The bottom line is that the FBI analyzed a pool of samples that very likely missed a huge portion of what should have been analyzed.

Validation

Very far into the process of developing the DNA tests, the FBI realized they needed to make an effort at validating their analysis. One of the validation attempts put one of the tests into huge question. Table 3 from their report shows this disappointing result:

Validation testing showed that for those results expected to be positive, no negative results were observed at or above the LOD for any of the genetic tests.[46] However, in the postvalidation testing, the negative rates were generally high. As shown in table 3, the negative rates for the postvalidation tests ranged from 0 percent to 43 percent for the undiluted samples from flask RMR-1029. (Appendix III breaks down the results of the replicate testing for each genetic test.)

Table 3: Sensitivity Results for Five Postvalidation Tests on Undiluted Samples from Flask RMR-1029

	Number		Sensitivity	
Genetic test	Replications from flask (positive samples)	Positive samples detected	Nonpositive results[a]	Estimated % negative rate[a]
A1	30	17	13	43.3
A3	30	29	1	3.3
D-1	30	23	7	23.3
D-2	30	24	6	20.0
E	30	30	0	0

Source: FBI, sensitivity statistics derived from 30 replicate samples selected from RMR-1029 using sample selection methods similar to the samples submitted to the FBI repository. | GAO-15-80

[a]Includes negative and inconclusive results as nonpositive results. The estimated negative rate is the number of non-positive results divided by the number of replications.

That’s a completely unacceptable result. The test called A1, when run 30 times in a row on material from the “smoking gun” RMR-1029, failed to detect the DNA variation in 13 of those tests. It gave a false negative in 43% of the tests when run on a known positive. And yet the FBI relied on this worthless test as part of the evidence to close the case.

Exclusion of Samples With One Inconclusive Test

If reliance on a worthless test isn’t disturbing

enough, the GAO report also dug out a point that was obscure in the NAS report. The FBI stated all along that in carrying out their analysis of the submitted cultures, they chose to eliminate from consideration any culture that gave an inconclusive result on any of the tests. But it turns out that there were some samples that definitely deserved further attention among those that were thrown out:

> The NAS report also raised concerns that the decision to remove samples with inconclusive or variant results contributed to the lack of completeness of the repository data. The report stated that a major concern was the restriction of its statistical analyses to the 947 samples that contained no inconclusive or variant results. Notably, the report showed that 4 of the 112 samples that were disregarded for having a single inconclusive or variant result scored positive for the three remaining genetic tests.

Think about that for just a minute. Recall that only 8 of the 947 included samples tested positive for all four changes. And yet there are four more potential samples that might have all four DNA changes that have three positives and one inconclusive among the 112 that had an inconclusive result.

Going back to find that information in the NAS report makes it even worse. It turns out that among the 947 samples included in the final analysis,there were only three that had three positive tests, so the four with three positives and one inconclusive among the excluded 112 is huge. Here is a table with those four samples:

In addition to the two 3-positive samples (+++) among the 947 samples, the four samples below also tested positive for 3 mutations (ordered by FBIR number):

052-026	+	+	+	inc	-	A1, A3, MRI-D
053-010	var	+	+	+	+	A3, MRI-D, IITRI-D, E
054-008	inc	+	+	inc	+	A3, MRI-D, E
054-066	+	Inc	+	+	+	A1, MRI-D, IITRI-D, E

Where did samples 052-026, 053-010, 054-008 and 054-066 come from? The falsely closed Amerithrax investigation needs to be reopened to follow these sloppily discarded leads.

ONLY REMAINING SENATOR PERSONALLY TARGETED BY TERRORIST ATTACK STILL BELIEVES IN CONSTITUTION

The Senate just voted down cloture on the USA Freedom Act, 58-42. Even while we disagreed on the bill, I extend sincere condolences to civil liberties allies who worked hard to pass this in good faith. I know you all have worked hard in good faith to pass something viable.

Several things about the vote were predictable (in fact, I predicted them in June). Just as one example, I noted to allies that if Jeff Flake — who had a great record on civil liberties while he was still in the House — did not support the effort, it would fail. Four Senators — cosponsors Mike Lee, Ted Cruz, and Dean Heller, plus Lisa Murkowski voted for cloture; Rand Paul did not. Bill Nelson voted against cloture as well (there are reports he is claiming it was a mistake, but given how closely this bill was whipped that would be … telling).

Equally predictable was the fear-mongering. GOP Senator after GOP Senator got up and insisted if the phone dragnet ended, ISIL would attack the country. None noted, of course, that the phone dragnet had never succeeded in preventing a terrorist attack. Pat Leahy made that point but it's one opponents of the dragnet need to make

in more concerted fashion.

Then there was a piece of news that neither side — supporter or opponent — seemed to want to mention. Dianne Feinstein revealed that at first 2 of 4 providers (presumably the fourth is T-Mobile though it could even be Microsoft, given that Skype is a more important phone carrier for international traffic) had refused to keep phone records, but that they had voluntarily agreed to do so for a full two years (this is at least a 6 month extension for Verizon, though may be significantly longer for cell calls).

The most dramatic part of the debate came after everyone left, when a frustrated Pat Leahy made the case for defending the Constitution. He recalled the anthrax letter addressed to him, on September 18, 2001, that killed a postal worker who processed it (~~another letter killed a Tom Daschle aide~~ see Meryl Nass' correction). "13 years ago this week, a letter was sent to me, addressed to me. It was so deadly, with the antrax in it that one person who touched the envelope—addressed to me, that I was supposed to open—They died!" Leahy reminded that the FBI had still not caught all the culprits for the attack. (That he believes that was first reported here in 2008; I believe FBI has, in fact, caught none of the culprits.) That attack targeting him personally, Leahy noted, did not convince him he had to abrogate the Constitution. "This nation should not let our liberties to be set aside by passing fears." Leahy said. "If we do not protect our Constitution we do not deserve to be in this body."

Senators like Marco Rubio got up and screamed about terrorists. But unless I'm mistaken, Pat Leahy is the only one remaining in the Senate who was personally targeted by a terrorist.

Maybe we ought to highlight that point?

Updated w/additions from Leahy's comments.