DOGE as a National Cyberattack

In the span of just weeks, the US government has experienced what may be the most consequential security breach in its history—not through a sophisticated cyberattack or an act of foreign espionage, but through official orders by a billionaire with a poorly defined government role. And the implications for national security are profound.

First, it was reported that people associated with the newly created Department of Government Efficiency (DOGE) had accessed the US Treasury computer system, giving them the ability to collect data on and potentially control the department's roughly $5.45 trillion in annual federal payments. Then, we learned that uncleared DOGE personnel had gained access to classified data from the US Agency for International Development, possibly copying it onto their own systems. Next, the Office of Personnel Management—which holds detailed personal data on millions of federal employees, including those with security clearances—was compromised. After that, Medicaid and Medicare records were compromised.

Meanwhile, only partially redacted names of CIA employees were sent over an unclassified email account. DOGE personnel are also reported to be feeding Education Department data into artificial intelligence software, and they have also started working at the Department of Energy.

This story is moving very fast. On Feb. 8, a federal judge blocked the DOGE team from accessing the Treasury Department systems any further. But given that DOGE workers have already copied data and possibly installed and modified software, it's unclear how this fixes anything.

In any case, breaches of other critical government systems are likely to follow unless federal employees stand firm on the protocols protecting national security.

The systems that DOGE is accessing are not esoteric pieces of our nation's infrastructure—they are the sinews of government.

For example, the Treasury Department systems contain the technical blueprints for how the federal government moves money, while the Office of Personnel Management (OPM) network contains information on who and what organizations the government employs and contracts with.

What makes this situation unprecedented isn't just the scope, but also the method of attack. Foreign adversaries typically spend years attempting to penetrate government systems such as these, using stealth to avoid being seen and carefully hiding any tells or tracks. The Chinese government's 2015 breach of OPM was a significant US security failure, and it illustrated how personnel data could be used to identify intelligence officers and compromise national security.

In this case, external operators with limited experience and minimal oversight are doing their work in plain sight and under massive public scrutiny: gaining the highest levels of administrative access and making changes to the United States' most sensitive networks, potentially introducing new security vulnerabilities in the process.

But the most alarming aspect isn't just the access being granted. It's the systematic dismantling of security measures that would detect and prevent misuse—including standard incident response protocols, auditing, and change-tracking mechanisms—by removing the career officials in charge of those security measures and replacing them with inexperienced operators.

The Treasury's computer systems have such an impact on national security that they were designed with the same principle that guides nuclear launch protocols: No single person should have unlimited power. Just as launching a nuclear missile requires two separate officers turning their keys simultaneously, making changes to critical financial systems traditionally requires multiple authorized personnel working in concert.

This approach, known as "separation of duties," isn't just bureaucratic red tape; it's a fundamental security principle as old as banking itself. When your local bank processes a large transfer, it requires two different employees to verify the transaction. When a company issues a major financial report, separate teams must review and approve it. These aren't just formalities—they're essential safeguards against corruption and error. These measures have been bypassed or ignored. It's as if someone found a way to rob Fort Knox by simply declaring that the new official policy is to fire all the guards and allow unescorted visits to the vault.

The implications for national security are staggering. Sen. Ron Wyden said his office had learned that the attackers gained privileges that allow them to modify core programs in Treasury Department computers that verify federal payments, access encrypted keys that secure financial transactions, and alter audit logs that record system changes. Over at OPM, reports indicate that individuals associated with DOGE connected an unauthorized server into the network. They are also reportedly training AI software on all of this sensitive data.

This is much more critical than the initial unauthorized access. These new servers have unknown capabilities and configurations, and there's no evidence that this new code has gone through any rigorous security testing protocols. The AIs being trained are certainly not secure enough for this kind of data. All are ideal targets for any adversary, foreign or domestic, also seeking access to federal data.

There's a reason why every modification—hardware or software—to these systems goes through a complex planning process and includes sophisticated access-control mechanisms. The national security crisis is that these systems are now much more vulnerable to dangerous attacks at the same time that the legitimate system administrators trained to protect them have been locked out.

By modifying core systems, the attackers have not only compromised current operations, but have also left behind vulnerabilities that could be exploited in future attacks—giving adversaries such as Russia and China an unprecedented opportunity. These countries have long targeted these systems. And they don't just want to gather intelligence—they also want to understand how to disrupt these systems in a crisis.

Now, the technical details of how these systems operate, their security protocols, and their vulnerabilities are now potentially exposed to unknown parties without any of the usual safeguards. Instead of having to breach heavily fortified digital walls, these parties can simply walk through doors that are being propped open—and then erase evidence of their actions.

The security implications span three critical areas.

First, system manipulation: External operators can now modify operations while also altering audit trails that would track their changes. Second, data exposure: Beyond accessing personal information and transaction records, these operators can copy entire system architectures and security configurations—in one case, the technical blueprint of the country's federal payment infrastructure.

Third, and most critically, is the issue of system control: These operators can alter core systems and

authentication mechanisms while disabling the very tools designed to detect such changes. This is more than modifying operations; it is modifying the infrastructure that those operations use.

To address these vulnerabilities, three immediate steps are essential. First, unauthorized access must be revoked and proper authentication protocols restored. Next, comprehensive system monitoring and change management must be reinstated—which, given the difficulty of cleaning a compromised system, will likely require a complete system reset. Finally, thorough audits must be conducted of all system changes made during this period.

This is beyond politics—this is a matter of national security. Foreign national intelligence organizations will be quick to take advantage of both the chaos and the new insecurities to steal US data and install backdoors to allow for future access.

Each day of continued unrestricted access makes the eventual recovery more difficult and increases the risk of irreversible damage to these critical systems. While the full impact may take time to assess, these steps represent the minimum necessary actions to begin restoring system integrity and security protocols.

Assuming that anyone in the government still cares.

This essay was written with Davi Ottenheimer, and originally appeared in Foreign Policy.

Tags: breaches, cybersecurity, hacking, national security policy

Posted on February 13, 2025 at 7:03 AM • 42 Comments

- not Like not Tweet

Comments

Mark • February 13, 2025 8:44 AM

Assuming that not enough people with power care – is this even recoverable assuming that Democrats or someone less 'burn it down' gets into power in the future? If the infection gets so deep over the next four years, would you ever go back without some sort of hard reset?

Nerijus • February 13, 2025 8:52 AM

"What makes this situation unprecedented isn't just the scope, but also the method of attack. Foreign adversaries typically spend years attempting to penetrate government systems such as these, using stealth to avoid being seen and carefully hiding any tells or tracks."

What makes you think this is not the foreign adversary attack? So far, Mump (term derived by historian Timothy Snyder) duo attacked allies (Canada/Denmark) or neutrals/friends (Panama/Mexico) and left adversaries (Russia/China) mostly untouched. To me this is a clear sign in whose pocket Mump are. And this is not only attack, but a coup, too.

Shoal Creek • February 13, 2025 8:59 AM

You're assuming that government (any government) is legitimate. It's not. Governments are basically racketeering gangs that fight each other for territory and try to give people the illusion that they chose to voluntarily participate. Mafias are just as legitimate, but without as much gaslighting. When a mafia starts to self-destruct, let it. It likely needs to be destroyed any way.

Bill • February 13, 2025 9:04 AM

This article is wrong on so many levels. First the president was voted in by a majority and is the head executive branch. He supports and oversees DOGE and has a team of people doing looking at what they are doing. He can give any person he chooses security clearance and access to government systems at his behest. He can also pardon anyone for any federal crime. Congress who is also majority

Republican seems to support this work. And the supreme Court also being majority Republican will likely side with him as well. So you're telling me that the president the head of the executive branch cannot go after a system which is obviously hacked and hijacked to go against him and the apparent will of the American people. This is not a coup the American people have been beaten down for the last 4 years and wanted this. Look at the depth of what they are finding. It doesn't bother you that our government pretty much funds all the mainstream news sources and gives disaster money away to non Americans? Regardless, our system of government was not created to have federal agencies undermine the will of American people.

Simon • February 13, 2025 9:06 AM

I've been wondering for a while whether (more likely how many) people have tried walking up to a federal department with some twenty-something men, saying "We're with DOGE, give us access", and seeing how far they get…

tfb • February 13, 2025 9:37 AM

@Shoal creek

By saying 'all governments are illegitimate' you are making what Erik Naggum called a 'one-bit mind' mistake: very obviously the legitimacy of a government is at the least a real number: some governments are more legitimate than others.

By say

Robin • February 13, 2025 9:46 AM

@Bill – you have missed the point completely. The essay is talking about national (cyber)security, not political legitimacy. It does not question whether it's the "will of the American people", but does highlight the fact that the actions are very significantly undermining the existential resilience of the USA.

Rob Keeney • February 13, 2025 9:52 AM

Breathless pearl clutching. This is what we elected Trump to do. There was no real oversight, no real guarantee that any of what these agencies were doing was actually beneficial to us. In fact, it's quite clear they've all been robbing us blind. All the security being torn down is around things that shouldn't exist in the first place. Burn it all to the ground and send them all to Gitmo.

fd • February 13, 2025 9:54 AM

If I'm reading this right, in the authors' preferred universe, "the Government" is not of, by, and for the people. It stands alone, impervious to inspection, control, or correction by those who, according to popular propaganda, "own" it.

No thanks.

F • February 13, 2025 9:54 AM

love Shoal Creek and Bill's comments. Clean the swamp!

Bill • February 13, 2025 10:05 AM

@robin you miss the point. We aren't concerned how they are doing it, we elected them to do this. We trust they are weighing the pros and cons of how they are going to do things. Schneier cannot prove more red tape = more security. We are also see the real and present danger of not doing this. The entire system has been highjacked to be used against the American people. That risk is much more dangerous in our eyes. Let's talk about how all these government agencies have been coopted to be used against the president and the American people. Let's talk about that as a security issue.

Yildo • February 13, 2025 10:14 AM

Well written and clearly explained. Thank you Davi, Bruce

Robert • February 13, 2025 10:18 AM

It looks like some of RFK's brain worms have infected Bill.

DownUnder'er • February 13, 2025 10:45 AM

@Bill : As a brazilian whose elections were effectively stolen to sit the leader of the largest theft in history back onto the presidential chair and whose freedoms are being heavily corroded in the last few years through the use of american taxpayer's money, I can only agree with you.

Of course the access to those Federal systems must be done responsibly. But I won't just believe Musk is being completely reckless or outright malicious without seeing any evidence simply because the very people who are being exposed like cockroaches claim that this is the way he's doing the work he was commissioned to do.

Right now I'm loving seeing those who were being paid to enforce censorship and push progressive agendas down our throats desperate now that the USAID money was cut.

@Robert: I assume you must not be aware of the USAID and NED scandal? American money that was supposedly being used to provide healthcare in poor countries but was actually funding censorship by the brazilian supreme court, a "transgender opera" in Colombia, venezuelan (a country not known for being very democratic, you know) electronic voting machines in Serbia, crafting narratives in media organizations everywhere? The list is endless and with abundance of proof. I know it sounds like a conspiracy theory but you can just look at the evidence, you know.

Me • February 13, 2025 10:46 AM

The owner of a company sends in auditors to make recommendations on staff and budget cuts. Owner tells them they have full access to anything they need.

Guess who complains the loudest? People about to have to justify their pointless (or corrupt) jobs.

Exactly the same, only the company is the Executive Branch.

I miss when you stayed out of politics.

Robert • February 13, 2025 10:49 AM

@DownUnder'er lol, yes I've seen that "evidence". Do they still have lead in the water where you are?

Andy • February 13, 2025 10:57 AM

"I miss when you stay out of politics" — hear, hear!

And those allegedly secure systems were repeated hacked: Treasure in December and OPM couple of years ago.

Moxieman • February 13, 2025 10:59 AM

"Breathless pearl clutching. This is what we elected Trump to do."

Which has nothing to do with not safeguarding information, reckless access, and firing experienced security personnel and replacing them with inexperienced personnel — laying the groundwork for future attacks.

The goals of the organizations have nothing to do with access and security.

Ishmael • February 13, 2025 11:04 AM

Sad times for the american experiment and great call out Bruce. No words for the trolls, hand waivers, and mickey mouse club members.

"If a wise man contends with a foolish man, Whether the fool rages or laughs, there is no peace."

Proverbs 29:9

John Pheedrus • February 13, 2025 11:04 AM

So now you're referring to a presidential appointed audit team as "attackers"? You're bias as a Democrat is on fully display here. The principles and implications are correct, but your attribution is based on links to MSM that have lied and continue to lie to the American people.
Try to be more objective.

smaug slayer • February 13, 2025 11:15 AM

The naked emporers are now riding the elepants in the room.
Good luck on future security. Skynet aka beast system – netscout x 1000 is implimented.
Good luck, prayed for everyone.

Gary Moore • February 13, 2025 11:19 AM

@Bill – you are part of the problem

Random Geek • February 13, 2025 11:24 AM

I read a couple of interesting articles which pertain to this discussion:
1) A Coup is In Progress in America
https://www.notesfromthecircus.com/p/a-coup-is-in-progress-in-america
2) The 'Tech-Industrial' Oligarchy Is Already Here
https://nymag.com/intelligencer/article/what-the-tech-industrial-complex-looks-like-under-trump.html

DownUnder'er • February 13, 2025 11:32 AM

@Robert: No, we never did. Brazil ia a country rich in water so it is actually pretty good while being relatively cheap.
But thank you for quickly showing that the only things you can add to this discussion are personal attacks and strawmen. That way I can safely ignore you knowing nothing useful will be lost.
@Me: exactly. They have very compelling reasons to claim that Musk did the worst atrocities imaginable. If the people from the former US government are anything (other than the same political spectrum) like their counterparts currently in charge over here there's no way a single word out of their mouths can be trusted without corroborating evidence, and even then you need to check for forgeries. Later at home I will follow the links in the story to confirm whether it is just claims or there are actual photos and videos of the allegations in the article, but I'm not holding my breath.

Bob • February 13, 2025 11:35 AM

All of my models are falling apart. Adding risk to the treasury, which has traditionally been considered risk-free for investment purposes. All of it breaks down when that assumption does.

Anonymous • February 13, 2025 11:42 AM

I am very confused about what this article is trying to say. Is it a cyberattack to vote for Donald Trump?

Anonymous • February 13, 2025 11:48 AM

Feels like talking about deniable encryption and the adversary got the right to torture you

Dancing on thin ice • February 13, 2025 12:12 PM

This being what may be the biggest security story ever or at least in a long time warrents further updates.
This week Time magazine writes about the 1960s Senator McCarthy red scare.

> a purge of State Department diplomats, including East Asia experts whose knowledge might have helped the U.S. avoid or mitigate its disastrous involvement in the Vietnam War

Expect long term ramifications.

Scott Lewis • February 13, 2025 12:14 PM

Some of these comments are ASTOUNDINGLY bizarre. Here we are on a SECURITY blog witnessing people who are security professionals, ostensibly, argue that there's no need for policies, procedures, access controls, security reviews and audits, and instead saying "we like the guy at the top, just do whatever he wants". What happened here exactly?

mark • February 13, 2025 12:25 PM

Love the right-wing and "libertarian" trolls, Bruce.

I've been in the streets in DC three times in the last two weeks, and my sign reads just that: Musk is making cyberwar against the US: JAIL HIM.

This is horrific. And as I spent 10 years at the NIH before retiring as a sr. sysadmin, and had to have at least a POT clearance, everything they've done breaks a ton of laws.

Robert • February 13, 2025 12:29 PM

@DownUnder'er yeah, also rich in strongmen dictators. I can see why you like Trump and Musk. I heard if you buy a Trump token, he'll send you a commemorative boot to lick. You should take advantage of that. I think I read about it on the same site you found your "evidence". lol.

Anonymous • February 13, 2025 12:49 PM

https://www.youtube.com/watch?v=RkmuI5W694o

Next, please tell us the security ramifications of outsourcing the development of critical systems to exhausted H1B employees in other countries. Or about storing critical data in "The Cloud".

Have popcorn, will travel.

Bill • February 13, 2025 12:54 PM

I see a lot of ad hominem attacks which signals this thread is likely to be locked soon.

Those of us who support this are essentially making these points.

1) it's not hacking if every branch of government supports this at the highest levels and doge is given authorization.

2) Bruce and everyone else here do not know the security measures doge has taken to secure the data. It is also not their business. We elected Trump who made it clear he would do this and defer to his judgement (which I know makes a great deal of you uncomfortable)

3) We know we have been manipulated and lied to in various ways for years by these agencies and DOGE uncovers more each day.

4) it's pretty much common knowledge now that Americans unknowingly funded the development of COVID.this is only one of many examples of abuse in these government agencies.

5) it's not a coup Trump won by majority vote and republicans won Congress by majority vote. The supreme Court has been appointed by elected officials.

6) these agencies were not elected and time and time again work outside of checks and balances and often interfere with proper oversight.

My question is how stupid would it be for Trump to allow these agencies who went after him and the American people to continue unchecked? Who elected these agencies? Where has the proper oversight been on them? Isnt the abuse and fraud they are finding worth it for the American people? Doesn't it make you upset to have been apart of a giant Truman show?

And finally, it actually doesn't matter what you think it's happening and will continue to happen no matter what you call it. No matter what you call people who support it. This is absolutely 100% what the majority of American people want.

Robert • February 13, 2025 1:01 PM

Listen to Bill complaining about ad-hominem attacks while his argumentation is pure authoritarian brain-rot. I'm sorry Bill, but I leave my good-faith arguments for people who are worthy.

K.S. • **February 13, 2025 1:09 PM**

Trump explicitly run on the platform of doing this and won majority. By trying to subvert the will of the people by attacking these efforts you are not that different from Jan6 rioters, but only insufficiently courageous to do so in person. Elections have consequences, this is one of them.

lurker • **February 13, 2025 1:12 PM**

I bet CRINK are laughing their elbows off at this.

Montecarlo • **February 13, 2025 1:15 PM**

Technically, it's a classified secret that government agencies are wasting money. In practice, however, it's more of an open secret.

Security protocols should be proportional to the risk – and exposing an open secret is relatively low risk. It is generally recognized that the President has the authority to request the executive branch to perform low risk tasks. For risky activities, of course, higher level approval would be required.

A.N • **February 13, 2025 1:26 PM**

Actions have consequences. Too many believe that American Exceptionalism is simply America flexing its muscles, not America being a true leader in the world. The admin is flexing its muscles in a way that is going to damage our country greatly, but that's what their voters wanted. They mistake hard power for true power, as much of America's power has been soft power.

Having someone come in and make drastic tech change to the historically most stable financial institution in the world? That's going to do extreme damage to the country's soft power due to the instability it may bring. More countries are going to stop attaching to the dollar and start going to China. This will greatly reduce America's soft power.

Chaos and such flexes is what our country keeps voting for because it feels manufactured pain from Fox News. When the treasury stops payments to medicare/medicaid, stops giving out tax returns, then the pain will become real. Sadly I think we need a breach of massive proportions that gives direct pain to the people for them to take any of this seriously and stop pointing at the imaginary scoreboard claiming that they are winning because the news says their team is ahead

Casey • **February 13, 2025 1:27 PM**

Scott, this article is getting linked to on social media. I would be really surprised if most of the people posting comments here know anything about computer security.

None of them try to dispute the technical points Bruce is making. They have to frame it as a political issue rather than a security issue because the points Bruce makes are valid regardless of one's political leanings.

Smart people are often wrong, stupid people never are. It's frustrating to accept that the sorts of people placing these comments will never have their minds changed by anything rational. They're not here for dialogue or to learn something. They just saw something on their social media feed that got them up in their feelings. Nothing that causes them discomfort by challenging their reality can go unremarked upon.

None of them provide evidence of anything. Not a single one. In fact, several of them go out of their way to say they refuse to read the articles being linked to because they know without reading them that they're "biased". It's all just hurt feelings, bad faith arguments and faux reasonableness.

Every totalitarian movement (on the right or left) must silence or discount experts. Experts get in the way of the state's monopoly on reality creation. The facts are biased, you see, and meritocracy makes mediocre people feel bad. So of course the expert is only saying that because they're a dirty liberal/capitalist/whatever.
Only the dictator can give you the unbiased truth. Trust him: he's doing this for your own good, unlike the experts who are just doing it for the money and power. It's incredible we ever made it out of the Dark Ages the first time, because the tactic works so well.

Clive Robinson • February 13, 2025 1:28 PM

@ ALL,
As some of you know I'm not from the US and for various reasons nolonger have any desire to visit. That said I can not avoid the effects of what the US Gov does or has done in it's name.
Depending on who you believe the US consumes around 50% of the worlds resources and generates some of the highest pollution levels. It also believes that it's law should apply to every place in the world, but has zero respect for anyone elses law.
So I can not ignore what goes on inside the US because it has direct effects on me, yet I have no right to say no by any process.
But I can observe and I can make comment for now.
So let's look at DOGE, the man in charge is allegedly a multi billionaire, but how did he make his money?
Well it turns out by "sucking on the Government welfare teat"…
But not just the US Gov teat, it turns out the Chinese Gov teat as well, in both cases in sums that total billions.
Is that subject to any "oversight" of course not, will the next load of welfare he gets be subject to oversight? Of course not.
As reported those teenagers and slightly older are not exactly experienced. However sone are known cyber criminals.
Correct me if I'm wrong, but I've been left with the impression that in many US States criminals are disbarred from public life in many ways. It's not only that they can not vote, nor are they allowed to hold government employment / posts, nor get the sort of security clearance required. The latter being true of federal government as well.
Now as the actions of these questionable folks can and does effect me directly, do you think I should be entitled to say if I agree with it or not?
Have a careful think before answering.

Anonymous • February 13, 2025 1:32 PM

Another related article at Lawfare:
https://www.lawfaremedia.org/article/musk-poses-cybersecurity-risks
And, yes, politics aside, the security implications of the way this is happening are troubling. Even if there are already exposures in some of these places, giving more people access, some of whom are unqualified, inexperienced, unknown, un-vetted, can't make things more secure. I expect big leaks of sensitive data, exploited by both criminals and adversaries.

Anonymous • February 13, 2025 1:32 PM

@Moxieman "The goals of the organizations have nothing to do with access and security."
Why should we care about the security of a harmful, criminal organization?