The Atlantic

Subscribe

TECHNOLOGY

THE GOVERNMENT'S COMPUTING EXPERTS SAY THEY ARE TERRIFIED

Four IT professionals lay out just how destructive Elon Musk's incursion into the U.S. government could be.

By Charlie Warzel and Ian Bogost

Illustration by The Atlantic. Source: Getty.

FEBRUARY 7, 2025
SHARE
SAVE

Listen

- 1.0x +

0:00

15:31

Produced by ElevenLabs and [News Over Audio (Noa)]() using AI narration. Listen to more stories on the Noa app.

If you have tips about the remaking of the federal government, you can contact Charlie and Ian on Signal at @cwarzel.92 and @ibogost.47.

Elon musk’s unceasing attempts to access the data and information systems of the federal government range so widely, and are so unprecedented and unpredictable, that government computing experts believe the effort has spun out of control. This week, we spoke with four federal-government IT professionals—all experienced contractors and civil servants who have built, modified, or maintained the kind of technological infrastructure that Musk’s inexperienced employees at his newly created Department of Government Efficiency are attempting to access. In our conversations, each expert was unequivocal: They are terrified and struggling to articulate the scale of the crisis.

Even if the president of the United States, the head of the executive branch, supports (and, importantly, understands) these efforts by DOGE, these experts told us, they would still consider Musk’s campaign to be a reckless and dangerous breach of the complex systems that keep America running. Federal IT systems facilitate operations as varied as sending payments from the Treasury Department and making sure that airplanes stay in the air, the sources told us.

Based on what has been reported, DOGE representatives have obtained or requested access to certain systems at the U.S. Treasury, the Department of Health and Human Services, the Office of Personnel Management, and the National Oceanic and Atmospheric Administration, with eyes toward others, including the Federal Aviation Administration. “This is the largest data breach and the largest IT security breach in our country’s history—at least that’s publicly known,” one contractor who has worked on classified information-security systems at numerous government agencies told us this week. “You can’t un-ring this bell. Once these DOGE guys have access to these data systems, they can ostensibly do with it what they want.”

Read: If DOGE goes nuclear

What exactly they want is unclear. And much remains unknown about what, exactly, is happening here. The contractor emphasized that nobody yet knows which information DOGE has access to, or what it plans to do with it.

Spokespeople for the White House, and Musk himself, did not respond to emailed requests for comment. Some reports have revealed the scope of DOGE's incursions at individual agencies; still, it has been difficult to see the broader context of DOGE's ambition.

The four experts laid out the implications of giving untrained individuals access to the technological infrastructure that controls the country. Their message is unambiguous: These are not systems you tamper with lightly. Musk and his crew could act deliberately to extract sensitive data, alter fundamental aspects of how these systems operate, or provide further access to unvetted actors. Or they may act with carelessness or incompetence, breaking the systems altogether. Given the scope of what these systems do, key government services might stop working properly, citizens could be harmed, and the damage might be difficult or impossible to undo. As one administrator for a federal agency with deep knowledge about the government's IT operations told us, "I don't think the public quite understands the level of danger."

Each of our four sources, three of whom requested anonymity out of fear of reprisal, made three points very clear: These systems are immense, they are complex, and they are critical. A single program run by the FAA to help air-traffic controllers, En Route Automation Modernization, contains nearly 2 million lines of code; an average iPhone app, for comparison, has about 50,000. The Treasury Department disburses trillions of dollars in payments per year.

Many systems and databases in a given agency feed into others, but access to them is restricted. Employees, contractors, civil-service government workers, and political appointees have strict controls on what they can access and limited visibility into the system as a whole. This is by design, as even the most mundane government databases can contain highly sensitive personal information. A security-clearance database such as those used by the Department of Justice or the Bureau of Alcohol, Tobacco, Firearms and Explosives, one contractor told us, could include information about a person's mental-health or sexual history, as well as disclosures about any information that a foreign government could use to blackmail them.

Even if DOGE has not tapped into these particular databases, *The Washington Post* reported on Wednesday that the group has accessed sensitive personnel data at OPM. *Mother Jones* also reported on Wednesday that an effort may be under way to effectively give Musk control over IT for the entire federal government, broadening his access to these agencies. Trump has said that Musk is acting only with his permission. "Elon can't do and won't do anything without our approval," he said to reporters recently. "And we will give him the approval where appropriate. Where it's not appropriate, we won't." The specter of what DOGE might do with that approval is still keeping the government employees we spoke with up at night. With relatively basic "read only" access, Musk's people could easily find individuals in databases or clone entire servers and transfer that secure information somewhere else. Even if Musk eventually loses access to these systems—owing to a temporary court order such as the one approved yesterday, say—whatever data he siphons now could be his forever.

Read: Trump advisers stopped Musk from hiring a noncitizen at DOGE

With a higher level of access—"write access"—a motivated person may be able to put their own code into the system, potentially without any oversight. The possibilities here are staggering. One could alter the data these systems process, or they could change the way the software operates—without any of the testing that would normally accompany changes to a critical system. Still another level of access, administrator privileges, could grant the broad ability to control a system, including hiding evidence of other alterations. "They could change or manipulate treasury data directly in the database with no way for people to audit or capture it," one contractor told us. "We'd have very little way to know it even happened."

The specific levels of access that Musk and his team have remain unclear and likely vary between agencies. On Tuesday, the Treasury said that DOGE had been given "read only" access to the department's federal payment system, though *Wired* then reported that one member of DOGE was able to write code on the system. Any focus on access tiers, for that matter, may actually simplify the problem at hand. These systems aren't just complex at the code level—they are multifaceted in their architecture. Systems can have subsystems; each of these can have its own permission structures. It's hard to talk about any agency's tech infrastructure as monolithic. It's less a database than it is a Russian nesting doll of databases, the experts said.

Musk's efforts represent a dramatic shift in the way the government's business has traditionally been conducted. Previously, security protocols were so strict that a contractor plugging a non-government-issued computer into an Ethernet port in a government agency office was considered a major security violation. Contrast that with DOGE's incursion. CNN reported yesterday that a 23-year-old former SpaceX intern without a background check was given a basic, low tier of access to Department of Energy IT systems, despite objections from department lawyers and information experts. "That these guys, who may not even have clearances, are just pulling up and plugging in their own servers is madness," one source told us, referring to an allegation that DOGE had connected its own server at OPM. "It's really hard to find good analogies for how big of a deal this is." The simple fact that Musk loyalists are in the building with their own computers is the heart of the problem—and helps explain why activities ostensibly authorized by the president are widely viewed as a catastrophic data breach.

The four systems professionals we spoke with do not know what damage might already have been done. “The longer this goes on, the greater the risk of potential fatal compromise increases,” Scott Cory, a former CIO for an agency in the HHS, told us. At the Treasury, this could mean stopping payments to government organizations or outside contracts it doesn’t want to pay. It could also mean diverting funds to other recipients. Or gumming up the works in the attempt to do those, or other, things.

In the faa, even a small systems disruption could cause mass grounding of flights, a halt in global shipping, or worse, downed planes. For instance, the agency oversees the Traffic Flow Management System, which calculates the overall demand for airspace in U.S. airports and which airlines depend on. “Going into these systems without an in-depth understanding of how they work both individually and interconnectedly is a recipe for disaster that will result in death and economic harm to our nation,” one FAA employee who has nearly a decade of experience with its system architecture told us. “‘Upgrading’ a system of which you know nothing about is a good way to break it, and breaking air travel is a worst-case scenario with consequences that will ripple out into all aspects of civilian life. It could easily get to a place where you can’t guarantee the safety of flights taking off and landing.” Nevertheless, on Wednesday Musk posted that “the DOGE team will aim to make rapid safety upgrades to the air traffic control system.”

Even if DOGE members are looking to modernize these systems, they may find themselves flummoxed. The government is big and old and complicated. One former official with experience in government IT systems, including at the Treasury, told us that *old* could mean that the systems were installed in 1962, 1992, or 2012. They might use a combination of software written in different programming languages: a little COBOL in the 1970s, a bit of Java in the 1990s. Knowledge about one system doesn’t give anyone—including Musk’s DOGE workers, some of whom were not even alive for Y2K—the ability to make intricate changes to another.

Read: The “rapid unscheduled disassembly” of the United States government

The internet economy, characterized by youth and disruption, favors inventing new systems and disposing of old ones. And the nation’s computer systems, like its roads and bridges, could certainly benefit from upgrades. But old computers don’t necessarily make for bad infrastructure, and government infrastructure isn’t always old anyway. The former Treasury official told us that mainframes—and COBOL, the ancient programming language they often run—are really good for what they do, such as batch processing for financial transactions.

Like the FAA employee, the payment-systems expert also fears that the most likely result of DOGE activity on federal systems will be breaking them, especially because of incompetence and lack of proper care. DOGE, he observed, may be prepared to view or hoover up data, but it doesn't appear to be prepared to carry out savvy and effective alterations to how the system operates. This should perhaps be reassuring. "If you were going to organize a heist of the U.S. Treasury," he said, "why in the world would you bring a handful of college students?" They would be useless. Your crew would need, at a minimum, a couple of guys with a decade or two of experience with COBOL, he said.

Unless, of course, you had the confidence that you could figure anything out, including a lumbering government system you don't respect in the first place. That interpretation of DOGE's theory of self seems both likely and even more scary, at the Treasury, the FAA, and beyond. *Would they even know what to do after logging in to such a machine?* we asked. "No, they'd have no idea," the payment expert said. "The sanguine thing to think about is that the code in these systems and the process and functions they manage are unbelievably complicated," Scott Cory said. "You'd have to be extremely knowledgeable if you were going into these systems and wanting to make changes with an impact on functionality."

But DOGE workers could try anyway. Mainframe computers have a keyboard and display, unlike the cloud-computing servers in data centers. According to the former Treasury IT expert, someone who could get into the room and had credentials for the system could access it and, via the same machine or a networked one, probably also deploy software changes to it. It's far more likely that they would break, rather than improve, a Treasury disbursement system in so doing, one source told us. "The volume of information they deal with [at the Treasury] is absolutely enormous, well beyond what anyone would deal with at SpaceX," the source said. Even a small alteration to a part of the system that has to do with the distribution of funds could wreak havoc, preventing those funds from being distributed or distributing them wrongly, for example. "It's like walking into a nuclear reactor and deciding to handle some plutonium."

Doge is many things—a dismantling of the federal government, a political project to flex power and punish perceived enemies—but it is also the logical end point of a strain of thought that's become popular in Silicon Valley during the boom times of Big Tech and easy money: that building software and writing code aren't just dominant skills for the 21st century, but proof of competence in any realm. In a post on X this week, John Shedletsky, a developer and an early employee at the popular gaming platform Roblox, summed up the philosophy nicely: "Silicon Valley built the modern world. Why shouldn't we run it?"

This attitude disgusted one of the officials we spoke with. "There's this bizarre belief that being able to do things with computers means you have to be super smart about everything else." Silicon Valley may have built the computational part of the modern world, but the rest of that world—the money, the airplanes, the roads, and the waterways—still exists. Knowing something, even a lot, about computers guarantees no knowledge about the world beyond them.

“I’d like to think that this is all so massive and complex that they won’t succeed in whatever it is they’re trying to do,” one of the experts told us. “But I wouldn’t want to wager that outcome against their egos.”

ABOUT THE AUTHORS

Charlie Warzel

Ian Bogost

Follow

Explore More Topics

Federal Aviation Administration, Silicon Valley