TechXplore

Is DOGE a cybersecurity threat? A security expert explains the dangers of violating protocols and regulations

February 8 2025, by Richard Forno

Credit: Pixabay/CC0 Public Domain

The Department of Government Efficiency (DOGE), President Donald Trump's special commission tasked with slashing federal spending, continues to disrupt Washington and the federal bureaucracy. According to published reports, its teams are dropping into federal agencies with a practically unlimited mandate to reform the federal government in accordance with recent executive orders.

As a 30-year cybersecurity veteran, I find the activities of DOGE thus far concerning. Its broad mandate across government, seemingly nonexistent oversight, and the apparent lack of operational competence of its employees have demonstrated that DOGE could create conditions that are ideal for cybersecurity or data privacy incidents that affect the entire nation.

Traditionally, the purpose of cybersecurity is to ensure the confidentiality and integrity of information and information systems while helping keep those systems available to those who need them. But in DOGE's first few weeks of existence, reports indicate that its staff appears to be ignoring those principles and potentially making the federal government more vulnerable to cyber incidents.

Technical competence

Cybersecurity and information technology, like any other business function, depend on employees trained specifically for their jobs. Just as you wouldn't let someone only qualified in first aid to perform open heart surgery, technology professionals require a baseline set of credentialed education, training and experience to ensure that the most qualified people are on the job.

Currently, the general public, federal agencies and Congress have little idea who is tinkering with the government's critical systems. DOGE's hiring process, including how it screens applicants for technical, operational or cybersecurity competency, as well as experience in government, is opaque. And journalists investigating the backgrounds of DOGE employees have been intimidated by the acting U.S. attorney in

Washington.

DOGE has hired young people fresh out of—or still in—college or with little or no experience in government, but who reportedly have strong technical prowess. But some have questionable backgrounds for such sensitive work. And one leading DOGE staffer working at the Treasury Department has since resigned over a series of racist social media posts.

According to reports, these DOGE staffers have been granted administrator-level technical access to a variety of federal systems. These include systems that process all federal payments, including Social Security, Medicare and the congressionally appropriated funds that run the government and its contracting operations.

DOGE operatives are quickly developing and deploying major software changes to very complex old systems and databases, according to reports. But given the speed of change, it's likely that there is little formal planning or quality control involved to ensure such changes don't break the system. Such actions run contrary to cybersecurity principles and best practices for technology management.

As a result, there's probably no way of knowing if these changes make it easier for malware to be introduced into government systems, if sensitive data can be accessed without authorization, or if DOGE's work is making government systems otherwise more unstable and more vulnerable.

If you don't know what you're doing in IT, really bad things can happen. A notable example is the failed launch of the healthcare.gov website in 2013. In the case of the Treasury Department's systems, that's fairly important to remember as the nation careens toward another debt-ceiling crisis and citizens look for their Social Security payments.

On Feb. 6, 2025, a federal judge ordered that DOGE staff be restricted to read-only access to the Treasury Department's payment systems, but the legal proceedings challenging the legality of their access to government IT systems are ongoing.

DOGE email servers

DOGE's apparent lack of cybersecurity competence is reflected in some of its first actions. DOGE installed its own email servers across the federal government to facilitate direct communication with rank-and-file employees outside official channels, disregarding time-tested best practices for cybersecurity and IT administration. A lawsuit by federal employees alleges that these systems did not undergo a security review as required by current federal cybersecurity standards.

There is an established process in the federal government to configure and deploy new systems to ensure they are stable, secure and unlikely to create cybersecurity problems. But DOGE ignored those practices, with predictable results.

For example, a journalist was able to send invitations to his newsletter to over 13,000 National Oceanic and Atmospheric Administration employees through one of these servers. In another case, the way in which employee responses to DOGE's Fork in the Road buyout offer to federal employees are collected could easily be manipulated by someone with malicious intent—a simple social engineering attack could wrongly end a worker's employment. And DOGE staff members reportedly are connecting their own untrusted devices to government networks, which potentially introduces new ways for cyberattackers to penetrate sensitive systems.

However, DOGE appears to be embracing creative cybersecurity practices in shielding itself. It's reorganizing its internal communications in order to dodge Freedom of Information Act requests into its work, and it's using cybersecurity techniques for tracking insider threats to prevent and investigate leaks of its activities.

Lacking management controls

But it's not just technical security that DOGE is ignoring. On Feb. 2, two security officials for the U.S. Agency for International Development resisted granting a DOGE team access to sensitive financial and personnel systems until their identities and clearances were verified, in accordance with federal requirements. Instead, the officials were threatened with arrest and placed on administrative leave, and DOGE's team gained access.

The Trump administration also has reclassified federal chief information officers, normally senior career employees with years of specialized knowledge, to be general employees subject to dismissal for political reasons. So there may well be a brain drain of IT talent in the federal government, or a constant turnover of both senior IT leadership and other technical experts. This change will almost certainly have ramifications for cybersecurity.

DOGE operatives now have direct access to the Office of Personnel Management's database of millions of federal employees, including those with security clearances holding sensitive positions. Without oversight, this access opens up the possibilities of privacy violations, tampering with employment records, intimidation or political retribution.

Support from all levels of management is crucial to provide accountability for cybersecurity and technology management. This is especially important in the public sector, where oversight and accountability is a critical function of good democratic governance and national security. After all, if people don't know what you're doing, they don't know what you're doing wrong.

At the moment, DOGE appears to be operating with very little oversight by anyone in position willing or able to hold it responsible for its actions.

Mitigating the damage

Career federal employees trying to follow legal or cybersecurity practices for federal systems and data are now placed in a difficult position. They either capitulate to DOGE staffers' instructions, thereby abandoning best practices and ignoring federal standards, or resist them and run the risk of being fired or disciplined.

The federal government's vast collections of data touch every citizen and company. While government systems may not be as trustworthy as they once were, people can still take steps to protect themselves from adverse consequences of DOGE's activities. Two good starting points are to lock your credit bureau records in case your government data is disclosed and using different logins and passwords on federal websites to conduct business.

It's crucial for the administration, Congress and the public to recognize the cybersecurity dangers that DOGE's activities pose and take meaningful steps to bring the organization under reasonable control and oversight.

Provided by The Conversation

Citation: Is DOGE a cybersecurity threat? A security expert explains the dangers of violating

protocols and regulations (2025, February 8) retrieved 27 March 2025 from
https://techxplore.com/news/2025-02-doge-cybersecurity-threat-expert-dangers.html