# The Government Shutdown Leaves Vulnerability in Cyber Security

Insights
1.22.19

While parts of the Government continue to be shut down over concerns about people crossing the border from Mexico into the United States, the cyber borders are at risk. Many government websites are not being monitored or maintained for security. Several websites have been rendered unsecured or inaccessible during the shutdown.

For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) put approximately 1,500 non-critical employees on furlough, or about 43 percent of its staff. Upon visiting DHS.gov, it provides the following message:

NOTICE: Due to the lapse in federal funding, this website will not be actively managed. This website was last updated on December 21, 2018 and will not be updated until after funding is enacted. As such, information on this website may not be up to date. Transactions submitted via this website might not be processed and we will not be able to respond to inquiries until after appropriations are enacted.

Employers are also unable to use E-Verify during the shutdown, which is the database where employers can presumably confirm that an employee is eligible to work in the United States. The Department of Homeland Security and U.S. Citizenship and Immigration Services announced that E-verify will not be maintained or updated during the shutdown, and employers cannot access their accounts to garner information.

In addition to the problems that people cannot access government websites for key information, is the concern that just attempting to access the sites poses a risk.

One concern is websites with expired TLS certificates, which leave sites unsecure. These certificates are the cryptographic protocols that provide authentication and data encryption between servers, machines and other applications operating over a network. Expired certificates bring the potential for cyber-attack. While the expired certificate may not directly expose the data, when one visits a page with an expired certificate there is a warning that the certificate is invalid, but often the user can still click through that warning and visit the site. This creates opportunities for hackers to intercept connections using fake TLS certificates.

Another concern is that with staff on furlough, some government networks will miss routine software updates and patch releases, which presents another opportunity for hackers to impact the government's network infrastructure. Not to mention that even once the shutdown ends, it will take some time to update and shore up these government websites to ensure security. Another concern is whether the government can even retain the talent of employees the longer the shutdown continues.

People should use caution when accessing government websites now and for the foreseeable future, even once the government is back open for business. If you get an expired certificate warning, do not click through it and access the site.  Ensure that your software and operating systems are up to date with protections against viruses and hackers.

## *Related People*

**Michelle I. Anderson**
Partner
504.529.3839
Email