Disclosure of security issue impacting DEA

Christopher Soghoian

Sun 2/28/2016 5:29 PM

To:BRET.M.STEVENS@USDOJ.GOV <BRET.M.STEVENS@USDOJ.GOV>;

Cc:privacy@usdoj.gov <privacy@usdoj.gov>;

Dear Mr Stevens,

I hope this email address is valid. It took a bit of work to identify the DEA's CISO, and then to locate your address (which I found via corporate registration records for your consulting company: http://atgsites.com/innovative_security_solutions_inc).

The DEA operates an online tip-form, through which individuals can report "possible violation of controlled substances laws and regulations. Violations may include the growing, manufacture, distribution or trafficking of controlled substances."

See: http://www.dea.gov/ops/submit.php

This website does not use HTTPS to protect the transmission of information. It should.

As you no doubt know, OMB has stated that every federal agency must use HTTPS, by default, for its entire public facing website by the end of 2016.
See: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

Per the OMB rule, agencies are supposed to prioritize "Web services that involve an exchange of personally identifiable information (PII), where the content is unambiguously sensitive in nature". An online form that solicits law-enforcement tips would seem to fall into this category.

I would greatly appreciate it if you could look into this issue and work to make sure that this website is secured appropriately.

On a more general note, I would also like to encourage you to post publicly contact information for your information security team, so that researchers and other individuals can responsibly disclose flaws such as this issue. This is a best practice followed by some federal agencies, widely adopted by those in the private sector, and promoted as a best practice by the Federal Trade Commission.

Thank you,

Christopher