DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

April 02, 2020

OIG-CA-20-015

MEMORANDUM FOR MARY G. RYAN
ACTING ADMINISTRATOR, ALCOHOL AND TOBACCO TAX AND TRADE BUREAU

FROM: Deborah L. Harker /s/
Assistant Inspector General for Audit

SUBJECT: Termination Memorandum – Audit of the Alcohol and Tobacco Tax and Trade Bureau's Network and Information System Security (A-IT-18-009)

In November 2017, we initiated an audit of the Alcohol and Tobacco Tax and Trade Bureau's (TTB) security controls over its network and information systems. The overall objective of our audit was to determine whether sufficient protections existed to prevent intrusions into TTB's network and information technology (IT) systems. We started this work in support of our ongoing oversight of the Department of the Treasury's (Treasury) compliance with the *Federal Information Security Modernization Act of 2014*, which requires among other things, that Federal agencies implement an agency-wide information security program for the information and the IT systems that support Treasury's operations. In this regard, we conduct periodic audits of network and information system security of Treasury's bureaus and offices.

The scope of our audit included a security assessment of TTB's Tax Major Application[1] (TMA), Regulatory Major Application[2] (RMA), and the general support system for TMA and RMA (hereinafter collectively referred to as "IT assets"). These IT assets were selected based on their significance to TTB's operations and the potential impact if there would be a disruption of service. We signed the Rules of Engagement (ROE) with TTB's Chief Information Officer on March 15, 2018, which established the roles and responsibilities for each party, the agreed upon times for penetration testing, the handling of data, and outlined our testing methodology, among other things. As part of our methodology, we conducted tests in the following phases: (1) discovery scans to verify potential targets; (2) a vulnerability assessment to scan for known security vulnerabilities; (3) exploitation/penetration testing of

[1] TMA is comprised of eight component systems that perform specific functions related to the collection of excise tax revenue from industry members.
[2] RMA is comprised of four component systems that track the status of incoming applications/requests/cases, provide a means to search, retrieve and view approved applications, and store a variety of information related to product formulations.

identified vulnerabilities to gain unauthorized access to TTB's IT assets; (4) and reporting of all activities during each test phase. To aid in our testing, we used commercial off-the-shelf scanning and penetration tools and publicly available IT security tools to perform our test. We performed our work primarily from TTB's facility in Washington, DC, between March and April 2018.

We performed ten separate scans of in-scope IT assets for potential vulnerabilities such as missing vendor patches, improper system configurations, application bugs, and factory default passwords. TTB's security controls blocked all scanning attempts. After TTB's Assistant Chief Information Officer (ACIO) identified our activity, the blocks were lifted to allow scans to continue. Our scanner identified potential vulnerabilities and rated 52 of them as critical and another 1,024 as severe. Critical vulnerabilities are those that are relatively easy for attackers to exploit and possibly take full control of TTB's IT assets. Severe vulnerabilities are harder to exploit and may not provide the same level of access to an IT asset as critical vulnerabilities. However, if exploited, they may cause similar types of damage as critical vulnerabilities. Our analysis confirmed that 10 critical vulnerabilities and 96 severe vulnerabilities were not duplicates, and therefore, considered unique. We attempted exploitation but failed as multiple layers of security controls immediately notified TTB's ACIO of our activity. As such, we determined that TTB's in-scope IT assets were sufficiently protected against intrusions at the time of our penetration testing in April 2018. Additionally, our scanner identified potentially obsolete operating systems (i.e. outdated and unsupported by vendors) on 176 individual devices. We confirmed with the ACIO that these devices were not running obsolete operating systems. That is, we verified that (1) non-obsolete operating systems were running on 148 devices, (2) the scanner identified 4 devices on the network that did not exist (i.e. false positives), and (3) the remaining 24 devices were decommissioned.

We are terminating this audit since we determined that TTB's in-scope IT assets were sufficiently protected against intrusions at the time of our penetration testing in April 2018, and due to the passage of time our testing results would no longer be applicable and useful to TTB management given the evolving nature of IT environments. That said, TTB's IT assets and infrastructure will be considered for future network and system vulnerability assessments and penetration testing as part of our annual planning process. Also note that *Audit of the Alcohol and Tobacco Tax and Trade Bureau's Network and Information System Security* (A-IT-18-009) will be removed from our *Monthly Status Report*.

We appreciate the courtesies and assistance provided by your staff. Should you have any questions concerning this memorandum, please contact me at (202) 927-5400 or Larissa Klimpel, Director, Cyber/Information Technology Audit, at (202) 927-0361.

cc: Robert J. Hughes, Chief Information Officer/Assistant Administrator
Information Resources