



OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Justice

(202) 514-3435 | oig.justice.gov

FOR IMMEDIATE RELEASE
April 1, 2019

DOJ OIG Releases Report on the FBI's Cyber Victim Notification Process

Department of Justice (DOJ) Inspector General Michael E. Horowitz today released a report examining the Federal Bureau of Investigation's (FBI) process for notifying and engaging with victims of cyber intrusions (cyber victims). The DOJ Office of the Inspector General (OIG) found issues with the completeness and quality of the data stored in the FBI's Cyber Guardian system — which tracks the production, dissemination, and disposition of cyber victim notifications — and identified problems with how the FBI conducted cyber victim notifications, both internally and in coordination with other government agencies.

The specific findings in the report released today include:

- **Reliability of Cyber Guardian Data.** The data in Cyber Guardian was unreliable due to typographical errors, a lack of controls that would prevent input errors, and the exclusion of many cyber victim notifications from especially sensitive investigations.
- **Cyber Victim Notifications.** The FBI was not informing all cyber victims of their rights under the Attorney General Guidelines for Victim and Witness Assistance (AG Guidelines). This occurred because: (1) the AG Guidelines do not appropriately address the specific needs of cybercrime victims; (2) there is no widely accepted definition of what constitutes a victim of cybercrime; and (3) there is currently no process for getting cybercrime victims' information from national security cases into the FBI's unclassified Victim Notification System — the system used to inform crime victims of their rights.
- **Victim Engagement.** We contacted 14 cyber victims to discuss their interaction with the FBI and found that the majority thought highly of FBI personnel and their interactions with them. However, some cyber victims complained about the timeliness of the notifications and whether the information provided by the FBI was adequate to remediate the threat to the victims' systems.
- **Coordination with Other Government Agencies.** We found several issues in instances where the FBI coordinates cyber victim notifications with other government agencies. Interagency conference calls for coordinating initial contact with victims were not conducted for all cyber incidents that required coordination by policy. Also, the Department of Homeland Security did not enter the cyber victim notifications that it

conducted into Cyber Guardian, contributing to the incompleteness of data. Finally, some notifications were delayed because of the need to protect the identities of cyber victims identified by another government agency.

- **CyNERGY System to Replace Cyber Guardian.** In 2019, the FBI plans to replace Cyber Guardian with a new system called CyNERGY, which was still under development at the time of our audit. We found that if the new system performs as intended, some of the issues found in Cyber Guardian should be addressed, but other issues will likely remain without additional fixes.

Today's report makes 13 recommendations to assist the FBI and the Department of Justice in improving the efficiency and effectiveness of the cyber victim notification process. The FBI and Department of Justice agreed with all 13 recommendations.

Report: Today's report is available on the OIG's website under "Recent Reports" and at the following link: <https://oig.justice.gov/reports/2019/a1923.pdf>.

Video: To accompany today's report, the OIG has released a 2-minute video featuring the Deputy Inspector General discussing the report's findings. The video and a downloadable transcript are available at the following <https://oig.justice.gov/multimedia/video-04-01-19.htm>.

###