



December 2024 | A-18-22-03400

The Organ Procurement and Transplantation Network IT System's Cybersecurity Controls Were Partially Effective and Improvements Are Needed

Why OIG Did This Audit

- HRSA oversees the contract for the Organ Procurement and Transplantation Network (OPTN) information technology (IT) system. The OPTN IT system contains data on every U.S. organ donor, transplant candidate, and recipient, as well as outcomes related to organ transplants. Securing the OPTN IT system with effective cybersecurity controls is important to the national organ transplantation system, its data, and the patients awaiting potentially life-saving organ donations.
- This audit examined (1) whether cybersecurity controls protecting the OPTN IT system were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise the OPTN IT system or data, and (3) the OPTN IT system's ability to detect attacks and respond appropriately.

What OIG Found

- Cybersecurity controls protecting the OPTN IT system were effective in preventing certain simulated cyberattacks (e.g., phishing), but the network monitoring of the OPTN IT system was not able to detect or respond appropriately to most of our simulated cyberattacks.
- We determined that it would likely take an attacker with a moderate level of sophistication to be able to compromise the OPTN IT system or data and cause significant harm.
- We identified 22 vulnerabilities associated with 16 cybersecurity controls, mostly related to network monitoring. The vulnerabilities occurred because certain federally required cybersecurity controls had not been implemented or were not operating effectively to prevent, detect, or mitigate some of our simulated cyberattacks.

What OIG Recommends

We made 4 recommendations to HRSA, including that it: require the OPTN IT system contractor to remediate the 22 vulnerabilities identified during our audit, verify that the vulnerabilities were remediated, require the contractor to improve network monitoring of the OPTN IT system, and implement procedures to help ensure that the OPTN IT system contractor is adhering to federally required cybersecurity controls policies and standards on a continuing basis. The full recommendations are in the report.

HRSA concurred with all four of our recommendations.