## Day-to-day expenses shouldn't count as cyber investments, the IG said.

Though the U.S. Postal Service’s investment strategies have strengthened its cybersecurity practice, the agency must produce a solid operational cyber budget to adequately steer the program and fund annual expenses, according to the Office of Inspector General’s [Semiannual Report to Congress](https://www.uspsoig.gov/sites/default/files/document-library-files/2019/2019_SARC_1_Spring.pdf) released this week.

In 2015, the agency approved millions in investments for Cybersecurity Decision Analysis Reports I and II. The total approved investment amounts are not publicly available but the OIG said it comprises “a capital investment, deployment investment expenses, and first-year operating expenses.”

Though the Postal Service uses the DAR process to “approve, fund, and monitor” operating expenses for cybersecurity investments, the OIG said daily operational expenses necessary to support cyber efforts should be managed differently.

“We found that expenses associated with day-to-day operations to sustain ongoing cybersecurity operations, such as rent, software licenses and services, and employee and contractor support, should not be considered investments per Postal Service investment policy,” the OIG said.

The internal watchdog said the Postal Service misclassified these operating expenses as investments because it did not execute long-term financial planning or adequately execute its cybersecurity program.

“Without an ongoing cybersecurity operating budget, the Postal Service may not be able to appropriately secure the enterprise to ensure uninterrupted service delivery, preserve customer and employee trust, and maintain competitive products in the digital marketplace,” it said.

The OIG also found that the Postal Service management faced challenges overseeing the DARs program because the agency uses multiple finance numbers to manage its investments. Additionally, the watchdog said there were millions in overspending on the DAR II program and the corporate information security office was unable to determine if it was a result of operational or deployment expenses because the office “did not track line item expenditures with sufficient detail” throughout the investment.

The OIG recommended that agency leadership produce a budget to better manage the cybersecurity program and to improve its tracking of DAR II spending against cash flow line items.

The OIG initially made those same recommendations in its [Cybersecurity Decision Analysis Reports Review](https://www.uspsoig.gov/sites/default/files/document-library-files/2018/IT-AR-19-002.pdf), published in November 2018. Agency officials agreed to the OIG’s directions at the time, saying its CISO would work with Finance and Planning to move its ongoing operating costs into new program/administrative budgets logically aligned with business functions and better track DAR II spending by January 31 of this year. The agreements and results of executing those plans were not mentioned in the Semiannual Report to Congress.