U.S. Department of Labor
Office of Inspector General
Audit

BRIEFLY...

STRONGER CONTROLS NEEDED OVER WEB APPLICATION SECURITY

November 14, 2019

WHY OIG CONDUCTED THE REVIEW

The Department of Labor (DOL) reported managing 72 publicly accessible web applications. These web applications provided gateways to DOL's information and services and therefore require adequate security to guard against a compromise of sensitive data and the unavailability of DOL's critical applications.

Concerned by the potential effects of comprised DOL web applications, we expanded upon our initial participation in a federal government wide review of securing publicly accessible web applications to understand better the extent of controls in place at the Department of Labor.

WHAT OIG DID

We conducted our review to answer the following question:

> Has DOL designed and implemented control activities that provide oversight of its publicly accessible web applications?

In performing the review, we surveyed DOL's information security officers about policies and procedures relevant to securing web applications and evaluated the Department's efforts to identify, assess, and resolve security vulnerabilities in its publicly accessible web applications.

READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2020/23-20-001-07-725.pdf

WHAT OIG FOUND

DOL did not implement sufficient control activities to monitor and secure its publicly accessible web applications. Specifically, the Department did not maintain a website inventory, remediate security vulnerabilities in a timely way, or implement security best practices.

Federal security standards require documenting and maintaining an accurate inventory of information system components, including web applications, to enforce security. DOL did not identify web applications as distinct system components to be inventoried for security purposes. Without an accurate inventory of web applications, DOL cannot ensure full oversight or quickly remediate weaknesses.

Further, one DOL agency did not remediate its highly-critical security weaknesses in a timely way. Specifically, we found that the agency canceled and reissued its corrective action plans, effectively restarting the timeframes. DOL has policies and procedures for remediating known weaknesses; however, this agency did not adhere to them, and DOL did not effectively monitor or validate the corrective actions. This lack of monitoring and validation unnecessarily prolonged exposure to known security weaknesses.

Lastly, DOL did not ensure its agencies utilized common government best practices for securing web applications, such as using secure programming techniques and web server configurations. Secure programming techniques guard against vulnerabilities within an application's programming. Secure web server configurations provide settings that, when applied, minimize security risks to the web application server. Applying best practices reduces the risk of security weaknesses in the system design.

WHAT OIG RECOMMENDED

We made three recommendations to improve the security of DOL's public-facing web applications by maintaining an inventory, increasing oversight and implementing secure programming best practices.

DOL generally concurred with our results and stated it recently established controls to correct the issues identified.