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

REPORT TO THE OFFICE OF THE
CHIEF INFORMATION OFFICER

STRONGER CONTROLS NEEDED OVER WEB APPLICATION SECURITY

DATE ISSUED: NOVEMBER 14, 2019
REPORT NUMBER: 23-20-001-07-725

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.

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

Gundeep Ahluwalia
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

This report presents the results of our review of the Department of Labor's (DOL) efforts to secure its publicly accessible web applications. The Department reported maintaining 72 publicly accessible web applications that provided a gateway to its information and services. Special attention is required to sufficiently secure publicly accessible web applications, and inadequate security can compromise sensitive data and interrupt applications critical to maintaining DOL mission operations.

Concerned by the potential effects of a compromise to DOL's web applications, we participated in a federal government wide review that focused on how agencies secure publicly accessible web applications. This review was led by the Counsel of Inspectors General on Integrity and Efficiency (CIGIE). As part of the CIGIE review, we analyzed DOL's efforts to identify, assess, and resolve security vulnerabilities on its publicly accessible web applications. We then expanded the CIGIE review to answer the following question:

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

We found weaknesses existed in the design and implementation of control activities established to ensure appropriate security and oversight of DOL's publicly accessible web applications.

As part of our review, we surveyed DOL agency information security officers (ISO) about policies and procedures relevant to securing web applications, and evaluated DOL's implementation and monitoring of those policies.

RESULTS

DOL did not design and implement control activities to provide oversight of its publicly accessible web applications. Specifically, we identified weaknesses in the design and implementation of the Department's control activities to ensure the following:

While the Office of the Chief Information Officer (OCIO) was responsible for providing oversight and security of DOL's information technology, including DOL's public-facing web applications, OCIO did not maintain a comprehensive inventory of the Department's public-facing web applications. Instead, OCIO relied on Departmental agencies to maintain their own inventory for web applications they managed. If DOL does not maintain a comprehensive inventory, it cannot identify and mitigate the risks posed by DOL web applications, and ultimately protect Department data from compromise.

We also found the OCIO was not ensuring the timely remediation of identified weaknesses in DOL's web applications and systems. Specifically, we found the Office of Public Affairs (OPA), delegated as the lead agency responsible for DOL's web applications, was not remedying its own identified security weaknesses in a timely manner. Additionally, we determined OCIO's monitoring of corrective actions did not ensure remediation was timely or sufficient to address the known security weaknesses.

Further, we found inconsistencies in agency policies for critical areas of web application development, including secure web programming and server configurations. DOL delegated these responsibilities to its agencies, some of which did not even develop the necessary policies, thereby increasing the risk that an attacker could successfully exploit a single weakness and gain access to sensitive Departmental information via its web applications.

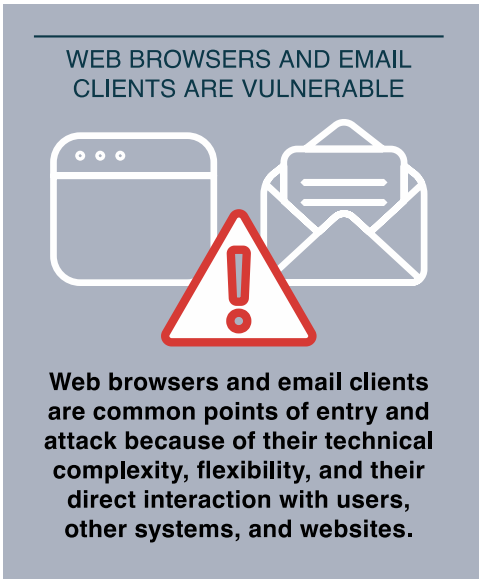
DOL will not be able to ensure availability, integrity, and confidentiality of public-facing web applications without establishing and implementing appropriate

security controls. Compromised websites serve as an entry point for intrusions into other internal networks and failure to implement adequate security for these web applications can lead to a compromise of sensitive data and the unavailability of DOL's critical applications.

DOL LACKED A COMPREHENSIVE INVENTORY OF WEB APPLICATIONS

DOL did not establish processes to identify and control its publicly accessible web applications. While OCIO developed policies and procedures for DOL agencies to follow in maintaining an inventory of systems, these policies and procedures did not include maintaining a comprehensive inventory of web applications.

One of the Center for Internet Security's top security controls focuses on application software security and references web applications as common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users, other systems, and websites.[1] Since publicly accessible web applications are the primary means for users to interact with DOL's information, these are potential targets for both code exploitation and social engineering.



Despite a 2008 OIG report[2] that recommended the development of such an inventory, we found OCIO did not maintain an enterprise-wide inventory of public-facing web applications for the purpose of identification and control. OCIO continued to delegate this responsibility to the agencies without maintaining oversight. Although we found some agencies had a process for tracking their web applications, 4 of the 9 agencies reviewed (44 percent) did not have such a process in place. See a depiction of these results in Figure 1.

[1] Center for Internet Security (CIS) Critical Security Controls Version 7, dated March 2018
[2] Web Application Security Report No. 23-08-002-50-598, dated September 2008

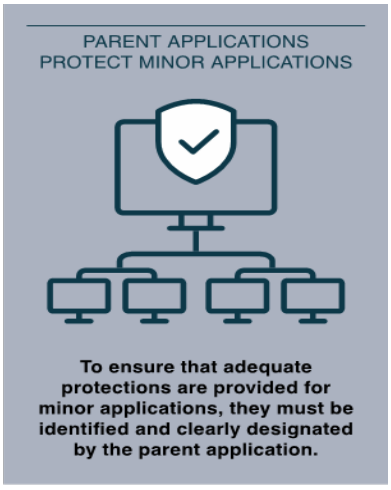
FIGURE 1: PROCESSES IN PLACE FOR TRACKING WEB APPLICATIONS

4 of the 9 agencies reviewed did not have a process in place for tracking their web applications

Source: ISO Survey Responses and OPA Test Results

Our 2008 report specifically recommended DOL CIO and the Assistant Secretary for Public Affairs coordinate efforts to secure DOL's public-facing web applications by establishing and implementing polices to increase accountability and improve management of key security controls, including completing an accurate inventory of all public-facing web applications. In an attempt to address this recommendation, OCIO performed a single inventory review in FY 2008. However, this was not established as a recurring control activity and only included web applications directly managed by OPA.

According to the National Institute of Standards & Technology (NIST)[3] SP 800-53 Revision 4, organizations are required to develop and document an inventory of their information system, including all system components.[4] This requirement is detailed in the DOL Computer Security Handbook (CSH), which specifies that in order to ensure adequate protections are provided for minor applications, such as web applications, these minor applications must be identified and clearly designated by the parent application. According to the DOL CSH, this is the



[3] National Institute of Standards and Technology (NIST) is a component of the Department of Commerce and the Federal Information Security Management Act assigns NIST the responsibility for developing standards and guidelines including security requirements for Federal Agencies.
[4] NIST SP 800-53 Revision 4 Control CM-8, Information System Component Inventory, dated April 2013

responsibility of an agency as part of its annual inventory assessment that is submitted to the OCIO.[5]

Not maintaining an accurate and complete inventory of public-facing web applications increases the risk that applications could exist in DOL's networked environment without the OCIO's knowledge, which could result in these applications not being scanned, patched, and monitored as part of OCIO's continuous monitoring program. Further, without continuous monitoring, security vulnerabilities could go undetected and DOL's information and networks would remain at greater risk of compromise.

PLANS FOR ACTION ESTABLISHED BUT REMEDIATION NOT TIMELY

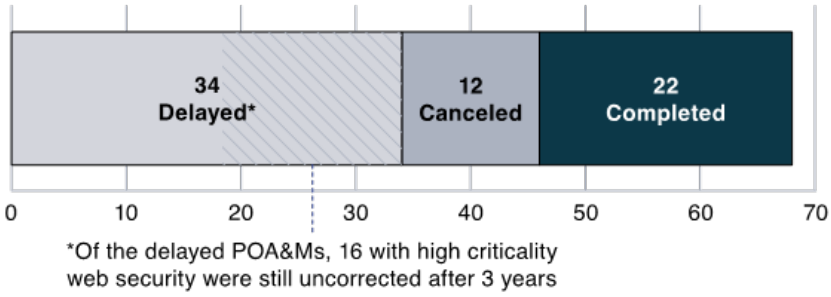
OPA established Plans of Action and Milestones (POA&Ms) for DOL's Web Production Environment System (DOL-WPES) to mitigate web application vulnerabilities but did not complete remediation efforts in a timely manner. The DOL-WPES is DOL's primary environment for the publishing of DOL internet and intranet services and the operational applications associated with these services.

While the OCIO monitors agencies' POA&Ms on a quarterly basis as part of its security oversight, this monitoring did not ensure OPA took timely action to mitigate identified vulnerabilities, which unnecessarily exposed DOL to ongoing security weaknesses. Further, we found OPA canceled POA&Ms without mitigating continuing weaknesses and lacked evidence to support the sufficiency of corrective action with regard to POA&Ms that were deemed complete.

At the time of our review, OPA had 68 POA&Ms for DOL-WPES. Our analysis showed that of the 68 total POA&Ms, 34 were delayed, 12 were canceled, and 22 were completed (see Figure 2 for a depiction of POA&M completion status).

[5] DOL Computer Security Handbook, Chapters 20 Inventory Methodology and Chapter 5 Configuration Management, Version 5.0, February 2014

FIGURE 2: COMPLETION STATUS OF THE 68 POA&Ms



Source: OIG Analysis of OPA's Plans of Action and Milestones

After we brought the lengthy delayed status of these POA&Ms to OPA's attention, OPA stated it was reevaluating and remediating the issues. Our follow-up analysis in August 2019 showed all 34 delayed POA&Ms were closed, and the majority were closed by decommissioning vulnerable applications or inheriting the controls from the DOL's general support system. OPA took on average 236 days to close the POA&Ms.

While OPA stated the original 12 canceled POA&Ms we identified had no impact on the system's security, we found OPA reopened those POA&Ms because the weaknesses persisted. By canceling and recreating the POA&Ms, OPA effectively reset the clock on implementing the security controls. However, OCIO policy states that, once canceled, a POA&M cannot be reopened. OPA did not follow this policy requirement when new POA&Ms were opened to address the same, unresolved weaknesses associated with the canceled POA&Ms. Further, OPA did not address the new POA&Ms in a timely way because OPA included these in the 34 delayed.

Further, of the 22 completed POA&Ms, 4 lacked sufficient evidence to support that the weakness had in fact been resolved, as required by OCIO policy.

Criticality of Delayed Actions and Milestones

For each identified weakness in a POA&M, the criticality of the weaknesses is assessed as high, medium, or low. Within the 34 delayed POA&Ms, we identified 16 weaknesses still uncorrected after 3 years that had been assessed as high criticality[6] to the application's security. Table 1 depicts the criticality of the vulnerabilities identified within the 34 delayed POA&Ms and reasons for delays:

[6] DOL's information security tool, Cyber Security Assessment and Management (CSAM) tool, assigned the criticality of the POA&Ms.

TABLE 1: REASONS FOR DELAYS

Criticality of Weakness	High	Medium	Low/Blank
Dependency on other task(s)	1	2	0
Original completion time underestimated	13	15	1
Funds not allocated/Insufficient Funds	2	0	0

Source: OIG Analysis of POA&M Detailed Report

These 16 high criticality POA&Ms were in the NIST control families of Risk Assessment (vulnerability scanning), System and Information Integrity (information input restrictions, validation and error handling), and Identification and Authentication (authentication management). For example, one of the 16 highly critical weaknesses identified during vulnerability scanning related to web applications being susceptible to well-known software code exploits known as Structured Query Language (SQL) injection and Cross-site scripting. SQL injection vulnerabilities are programming codes inserted into a web application's data entry field that allow for the execution of malicious programming code. Cross-site scripting consists of vulnerabilities that arise when permissions from one user's request to a web application are copied or echoed into another's request, allowing the malicious application unauthorized access to the system.

DOL policy required each DOL agency to report its POA&Ms on a quarterly basis so OCIO could monitor agency-wide remediation efforts through the semiannual review process. According to specific POA&M policy guidance issued by OCIO, steps for the remediation of POA&M weaknesses need to be specific, measurable, and attainable in a timely manner. Additionally, POA&Ms were to be closed only after all milestones had been completed, steps had been taken to resolve the weakness, and the evidence to support the milestone closures had been uploaded in DOL's security management tool. Based on our review of OPA's POA&Ms, we identified several instances where these criteria were not followed.

OCIO did not effectively monitor remediation efforts through the semiannual review process, which should provide a means to manage risk while complying with applicable laws, regulations, and policies. Effective monitoring would have exposed OPA's failure to remediate its POA&Ms in a timely manner. The inability to remediate outstanding issues or weaknesses in a timely manner leaves DOL unnecessarily at risk of security exploitation, which could compromise agency information and lead to a loss of public trust.

POLICIES AND PROCEDURES DID NOT SECURE DOL'S PUBLIC WEB APPLICATIONS

OCIO did not ensure policies and procedures for web applications were consistently developed and implemented by its agencies. As DOL's lead organization in securing its systems, including web applications, OCIO developed and issued policies for agencies to implement. These policies should have aligned with NIST SP 800-53 rev 4 baseline security requirements. Weaknesses in developing and implementing policies for secure programming and operating environments can impact the Department's ability to standardize the practice of prioritizing the identified security vulnerabilities, which is critical to reducing the risk of a malicious actor successfully exploiting a single weakness and gaining access to sensitive Departmental data.

In gaining an understanding of DOL's policies and procedures for securing web applications, we obtained OPA's policies and procedures for securing web applications. We analyzed the OPA IT security policies and procedures against 10 high-risk areas identified for the CIGIE review. Additionally, we surveyed 8 agency ISOs regarding their agencies' policies and procedures in the same areas of review.

Through our analysis, we identified that critical web application security policies and procedures were only partially developed for the following: 1) comprehensive web application inventory; 2) secure software programming of web-based applications; 3) web application consolidation; and 4) hardening web server operating environments. See Table 2 for the results of the survey and the OPA analysis:[7]

[7] Areas selected by HUD-OIG, lead for the CIGIE review, using a NASA OIG report: Security of NASA's Publicly Accessible Web Applications, dated July 10, 2014.

TABLE 2: ANALYSIS OF AGENCY POLICIES AND PROCEDURES

Area/Process Description	8 Agencies Results*	OPA Results
Web based application security policies and procedures (NIST 800-53 controls)	All	Yes
Secure Software Programming of Web based applications	5	Yes
Hardening web server operating environments	5	No
Scanning, tools used, and frequency	All	Yes
Identifying vulnerabilities and patching web based applications	All	Yes
Security enhancing lifecycle processes (SDLC)	All	Yes
Inventory Processes for tracking Web based applications	4	Yes
User account logging policy	All	Yes
User account password policy	All	Yes
Web application consolidation efforts in place	5	Yes

*Of the eight ISO's surveyed, the number of ISO's that responded and provided supporting documentation.

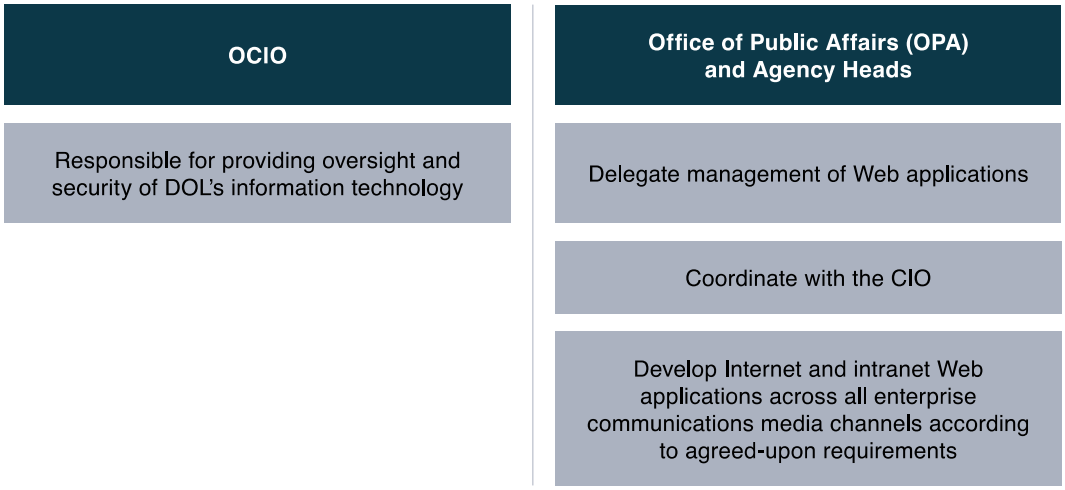
Source: OIG Analysis of ISO survey results and OPA Testing

NIST SP 800-53 controls over security engineering and configuration call for security requirements in the following areas: specification, design, development, implementation, and modification of the information system. NIST SP 800-53 also details requirements for the establishment and documentation of security configuration settings using checklists that reflect the most restrictive mode consistent with operational requirements.[8] In implementing these NIST controls, DOL's CSH required agencies to apply guidance consistent with NIST SP 800-53.[9]

While OCIO was responsible for providing oversight and security of DOL's information technology, DOL Secretary's Order 2-2005[10] delegated management of web applications to OPA and agency heads (see Figure 3 for a depiction of these delegated responsibilities). In this order, agency heads and OPA were required to coordinate with the OCIO, but were responsible for developing intranet web applications across all enterprise communications media channels according to agreed-on requirements. Exceptions to this responsibility occur when agency control over the development of such applications is established by law or is authorized jointly by an agency and OPA upon agency request.

[8] NIST SP 800-53 Revision 4 Control SA-8, Security Engineering Principles, and CM-6, Configuration Settings, Dated April 2013
[9] DOL Computer Security Handbook, Volume 15 "System and Services Acquisition" section 3.2.4 Design and Implement Using Security Engineering Principles, Version 5.0, February 2014
[10] Secretary's Order 2-2005, Delegation of Authority and Assignment of Responsibility for DOL Enterprise Communications Initiative dated September 30, 2005

FIGURE 3: ROLES AND RESPONSIBILITIES



Source: Secretary's Order 2-2005

Although OCIO had ultimate responsibility for the security of DOL information technology, including its public-facing web applications, OCIO did not provide clear and consistent policy and procedural guidance to OPA and other Departmental agencies for developing and securing public-facing web applications. In the absence of such guidance, agency policies did not ensure secure management of web applications and web server operation systems, increasing the risk that DOL web applications and the servers that hosted them could contain weaknesses that could be exploited by adversaries.

For example, in 2016 the Internal Revenue Service was the target of a malware attack through the E-file website that compromised electronic tax-return credentials and allowed the attacker to gain access to 101,000 social security numbers. Additionally, an attacker successfully hacked DOL's Substance Abuse Information Database web application in August 2006, exploiting the common vulnerability SQL injection. The attacker altered fields in the web application's underlying database, resulting in the web page's defacement. This review found DOL had yet to remediate the causes that allowed this intrusion to occur.

CONCLUSION

OCIO's control activities did not ensure proper security and oversight of its publicly accessible web applications. Specifically, OCIO did not maintain a website inventory, remediate security vulnerabilities in a timely manner, or implement security best practices. Since publicly accessible web applications are the primary means for users to interact with DOL's information, these sites are vulnerable to both code exploitation and social engineering. As such, DOL's weak controls over its publicly accessible web applications put DOL data and networks at risk of compromise.

OIG'S RECOMMENDATIONS

We recommend the Chief Information Officer:

1. Establish and maintain a comprehensive inventory of web applications, identifying which applications are public-facing and contain sensitive information. Such an inventory should itemize all system interfaces with the web application for the purpose of ensuring the applications are properly secured and to enable a quick response when new vulnerabilities are encountered.

2. Review and update DOL POA&M policy to ensure agency corrective actions and timeframes are implemented.

3. Establish and verify the implementation of Department-wide policies and procedures specific to associated risks to web applications, securing web servers, and web application programming.

SUMMARY OF THE CHIEF INFORMATION OFFICER'S RESPONSE

In response to the report, the CIO generally agreed with our results and stated the OCIO recently implemented policy and guidance that should resolve the recommendations in this report. However, the information provided by the OCIO as of the date of its response did not sufficiently address our recommendations. While the response identified OCIO relied on Department of Homeland Security to identify and secure its web servers and applications, the inventory of 72 public facing web applications initially provided by the OCIO – compiled manually from OCIO data calls to the agencies - remains the only web application inventory provided to the auditors to date. We requested updates on several occasions, as recently as September 2019, to the information presented in this report. The OCIO confirmed the accuracy of the information presented, including the accuracy of the 72 websites listed on its initial inventory provided. While the OCIO has since raised issue with the number of web applications reported by the OIG, the OCIO has not provided the OIG with an updated inventory of DOL web applications to update the previously confirmed data.

Additionally, the policies and procedures issued by the CIO still do not address the risks specifically associated with securing web applications or sufficiently reference federal guidance such as NIST SP 800-44 *Guidelines on Securing Public Web Servers* and NIST SP 800-95 *Guide to Secure Web Services*. As such, we will continue to work with the OCIO to address the recommendations made in this report. The CIO's written response to our draft report is included in its entirety in Appendix B.

We appreciate the cooperation and courtesies the Office of the Chief Information Officer and Office of Public Affairs extended us during this review. OIG personnel who made major contributions to this report are listed in Appendix C.

Elliot P. Lewis
Assistant Inspector General for Audit

APPENDIX A: SCOPE, METHODOLOGY, & CRITERIA

SCOPE

Our scope covered DOL policies and procedures specific to maintaining and securing its public-facing web applications. Additionally, this review utilized data for the period FY 2012 – 2019. Our work was conducted primarily with OCIO and OPA headquarters personnel located in Washington, DC.

METHODOLOGY

We performed this review in accordance with the Quality Standards for Inspection and Evaluation issued by CIGIE. Those standards require we plan and perform the review to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

This review expanded upon the work we conducted as part of a CIGIE IT Subcommittee cross-cutting project. The purpose of our evaluation review was to leverage the information obtained as part of the CIGIE project and determine if DOL designed and implemented control activities that provide oversight of its publicly accessible web applications.

Analysis included a review of DOL, OCIO, and OPA policy and a survey approach to obtain additional information from agency ISO's. An inventory of publicly accessible web applications was developed through the use of a data call sent out to all agency ISO's. Based on this approach, it was determined that there were 72 publicly accessible web applications.

CRITERIA

- Secretary Order 02-2005 Delegation of Authority and Assignment of Responsibility for DOL Enterprise Communications Initiative, September 30, 2005
- Secretary Order 03-2003 Update of Delegation of Authority and Assignment of Responsibility to the Chief Information Officer, May 26, 2003
- Inspector General on Integrity and Efficiency (CIGIE), Standards for Inspection and Evaluation, January 2012

- DOL Computer Security Handbook DOL Computer Security Handbook, Version 5.0, February 2014
- NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- DOL-OCIO Plan of Action and Milestone (POA&M) Management Guide, Version 1.0, May 2015
- GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 10, 2014
- GAO, *Assessing the Reliability of Computer-Processed Data*, GAO-09-680G, July 2009

PRIOR COVERAGE

During the last 10 years, we issued one report of significant relevance to the subject of this report:

> *Web Application Security Report No. 23-08-002-50-598, dated September 2008*

The Council of the Inspectors General on Integrity and Efficiency issued a report of significant relevance to the subject of this report:

> *Web Applications Security Cross-Cutting Project – A Federal Government Assessment of Publicly Facing Web Applications, date October 2017*

The Government Accountability Office (GAO) did not issue any reports of significant relevance to the subject of this report.

APPENDIX B: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA Digitally signed by GUNDEEP AHLUWALIA Date: 2019.10.24 17:06:09 -04'00'

SUBJECT: Management Response to the DRAFT REPORT – Stronger Controls Needed Over Web Application Security, Draft Report No. 23-20-001-07-725

This memorandum addresses the above-referenced DRAFT REPORT – *23-20-001-07-725 Stronger Controls Needed Over Web Application Security* issued to the DOL Chief Information Officer (CIO) on October 3, 2019, for management's review and response.

DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve security for our information systems and data. OCIO management concurs that at the completion of the OIG Field Work in 2016 the Notice of Finding and Recommendation was valid. However, since that time, the DOL's IT environment has significantly changed and the security posture matured. OCIO contends that the changes and improvements affect the conditions related to this NFR to the point that they can be closed. Those changes and improvements include:

1. As part of the continuous monitoring program to address security vulnerabilities relating to public facing websites, DOL's internet perimeter is scanned by DHS. These scans capture and provide a list of all DOL websites. DHS also provides OCIO weekly cyber hygiene reports which indicate any related identified vulnerabilities. Agencies are required to reconcile their web sites to the list provided by the DHS. Identified vulnerabilities (to systems containing sensitive and non-sensitive information) are remediated accordingly. This process provides assurance that DOL's websites and by extension web applications are adequately secured and in alignment with the DHS reports.
    - See attached DHS Cyber Hygiene Assessment Report (cyhy-DOL-2019-10-06T231652+0000.pdf)
    - See attached DOLCSIRC alert to address the weaknesses (DOLCSIRC-N-20-006 (DHS Cyber Hygiene Scan-results) Update 1 TLP AMBER.msg)

2. The information security continuous monitoring (ISCM) approach has undergone several revisions with much emphasis on POA&M management within the Department's information security and risk management program documentation. The Department's POA&M management process (POA&M Management Guide v1.2) has been enhanced to ensure corrective actions and time frames are implemented according to policy. This process has increased the review frequency, realigned the review to include qualitative and quantitative performance measures of POA&M activities and use the information to make appropriate adjustments as needed, follow up and reporting to management.
    - See attached POA&M Management Guide v1.2

3. As it relates to establish and verify the implementation of Department-wide policies and procedures specific to associated risks to web applications, securing web servers, and web application programming; while the policies do not explicitly reference "web applications", the Computer Security Handbook Edition 5 (CSH 5) volumes below are among the Department's policies and procedures that address hardening web server operating environment:
    - Access Control Protection Policy, Procedure and Standards, Version 1.1 (Last Update 8/14/2018)
    - Audit and Accountability Policy, Procedures, and Standards, Version 1.0, (Last update 3/31/2016)
    - Identification and Authentication Policy, Procedures, and Standards, Version 1.0, (Last Update 6/5/2018)
    - Configuration Management Policy, Procedures, and Standards, Version 1.0, (Last Update 8/27/2018)

    In particular, CSH Volume 5 – Configuration Management, section 3.1.5 states "***DOL's required minimum standards on configuring settings for information technology products are as follows:…*** *FISMA, section 3544(b)(2)(D)(iii), requires each federal agency to develop "minimally acceptable security configuration requirements" and ensure compliance with them. All security configuration standards issued as part of this volume comply with FISMA and the Department of Labor Manual Series (DLMS) Chapter 9 Section 400 (407)(A)(2)(b) and are based on the criteria listed below:…*

    c. *In the absence of NIST guidance to address a specific technology, common secure configurations (also referred to as a NIST approved security configuration checklist (such as but not limited to the United States Government Configuration Baseline (USGCB), Security Content Automation Protocol (SCAP), Common Configuration Enumeration (CCE)), lockdown and hardening guides, security reference guides, security technical implementation guides) must be utilized."*

    Management contends that this policy applies to and addresses associated risks to all services including websites and web applications.

OCIO believes that all the above actions are sufficient to close the recommendations. In addition, Management recommends the OIG revise the opening statement "The Department of Labor (DOL) managed 72 publicly accessible web applications as of March 2019", to reflect that this was the state of the inventory as of 2016 not 2019.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202)-693-4446 or have your staff contact Paul Blahusch, Chief Information Security Officer, at Blahusch.Paul.E@dol.gov or (202) 693-1567.

cc: Bryan Slater, Assistant Secretary for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Paul Blahusch, Chief Information Security Officer (CISO)
Scott Davis, Deputy Chief Information Security Officer (CISO) D/CISO
Muhammad Butt, Division Director, Information Security Policy & Planning (ISSP)

APPENDIX C: ACKNOWLEDGEMENTS

Key contributors to this report included:

Stephen Fowler, IT Audit Director
Ethan Iczkovitz, IT Audit Manager
Benjamin Brady, Information Technology Specialist
Naomi Reynolds, Auditor
Carmen Wilson, Auditor

REPORT FRAUD, WASTE, OR ABUSE
TO THE DEPARTMENT OF LABOR

Online
http://www.oig.dol.gov/hotline.htm

Telephone
(800) 347-3756 or (202) 693-6999

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Room S-5506
Washington, DC 20210