U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

July 31, 2015

MEMORANDUM FOR: DAWN M. LEAF
Chief Information Officer

FROM: ELLIOT P. LEWIS
Assistant Inspector General for Audit

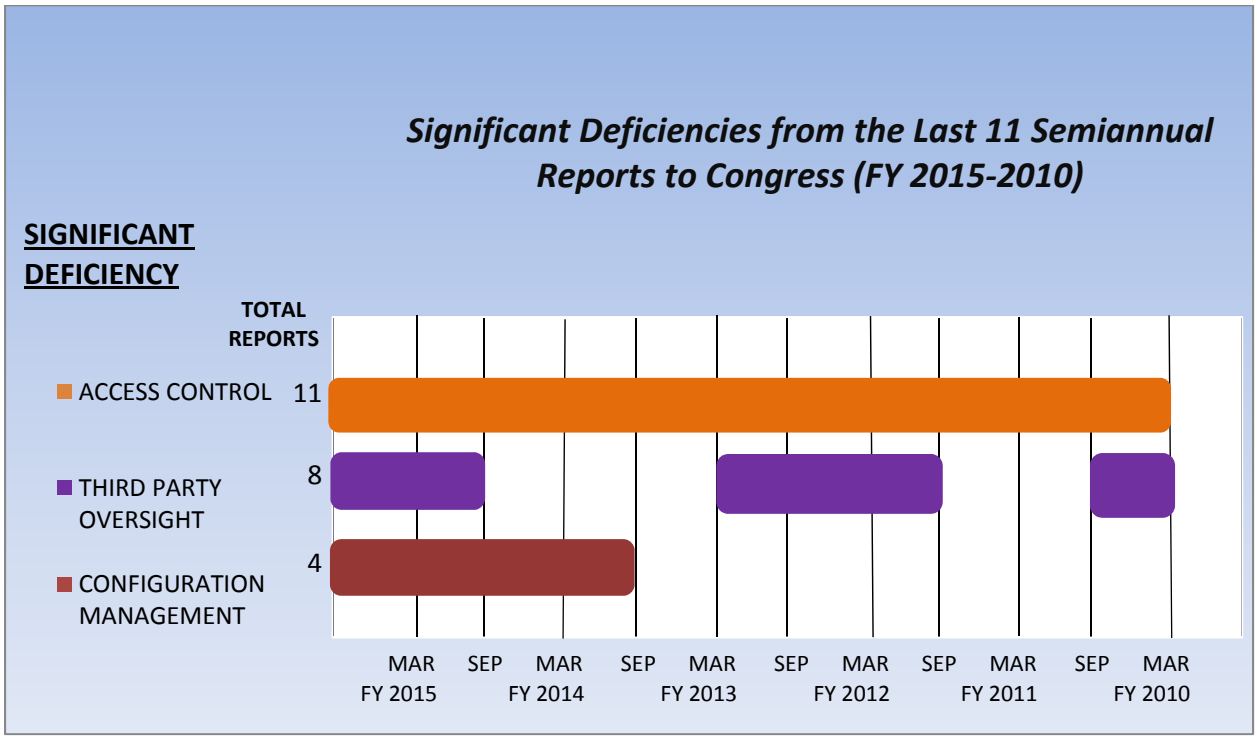
SUBJECT: Information Security Concerns
Report Number: 23-15-009-07-725

In light of recent events involving serious breaches of government data systems, this memorandum highlights three significant deficiencies that have been repeatedly identified in our reports on the Department of Labor's (DOL) information security program. DOL must make it a high priority to mitigate these serious security vulnerabilities to its information systems. These three significant deficiencies are:

- Access controls
- Third-party oversight
- Configuration management

DOL has initiated corrective actions to address these deficiencies as OIG has identified them during our annual Federal Information Security Management Act (FISMA) testing of subsets of DOL systems. However, this trend of recurring deficiencies is indicative of systemic issues that require an overall strengthening of DOL's information security program to prevent future occurrences.

The following chart shows when we have raised these significant deficiencies over the past five years.



In addition to making recommendations related to the three significant deficiencies described above, OIG has made recommendations to correct control deficiencies across numerous control families, including contingency planning, security assessment and authorization, risk assessment, and incident response.

Summary of Three Significant Deficiencies

Access Control

One of the most frequently identified deficiencies has been in the area of access controls. Access control deficiencies have been cited in each of the 11 Semiannual Reports to Congress that OIG has issued over the past 5 years. Access controls are preventative measures established for the purpose of determining the allowed activities of legitimate users and restricting users' access to system resources.

OIG has repeatedly recommended DOL improve this important control to prevent unauthorized access to DOL systems and applications. OIG recommended in September 2012 that DOL continue to plan and implement logical access via Personal Identity Verification (PIV) cards to achieve compliance with Department of Homeland Security Presidential Directive 12. DOL only recently began implementing this requirement in response to the Office of Personnel Management breach. Had DOL implemented the requirement earlier, it could have prevented unauthorized access to DOL's computer networks and systems by 11 separated employees who still had active accounts after their departure. Moreover, by not implementing this control earlier DOL

unnecessarily exposed itself to greater risk of unauthorized access. Finally, if the rollout had not been delayed, DOL may have been better positioned to more efficiently use the resources necessary to accomplish this significant effort more timely and with less disruption to agencies.

Deficiencies Identified in the PIV System

Deficiencies identified in the PIV system related to issuance of PIV cards and creation of individual profile information and pins:

- September 7, 2012 – OIG's Alert Memorandum, *DOL Needs to Take Immediate Action to Correct Security Weaknesses in the PIV-II System,* identified serious control deficiencies in the areas of account management, system login, system privileges and agreements, system security assessments, system training, contingency planning, system security plan, system rules of behavior, and configuration management. Taken individually, these deficiencies were very serious. Taken as a whole, their impact on the PIV-II security program placed DOL at a high risk for harm to infrastructure, systems, data, employees, contractors, and visitors.

- March 29, 2013 – OIG's report, *Department's Information Technology Security Program Is Weakened by Deficiencies*, noted PIV-II security program weaknesses continued as a significant deficiency for the DOL IT security program because of the substantial and pervasive risks to the confidentiality, integrity, and availability of mission critical and sensitive data.

The importance of the PIV-II security program cannot be understated. The program plays a key role in protecting DOL's infrastructure, including data, other systems, and people from potential harm caused by unauthorized access. Although DOL is now implementing logical access via PIV cards, it will need to ensure all aspects of PIV card issuance and maintenance are properly administered in order to ensure the effectiveness of this control.

Other Access Control Deficiencies Identified

Additional access control deficiencies identified include improper account management, unauthorized privileged users, undocumented rules of behavior, no lock-out after unsuccessful log-in attempts, and outdated system security plans. These deficiencies and others have been identified in numerous reports:

- March 30, 2010 – OIG's report, *Actions Required to Resolve Significant Deficiencies and Improve DOL's Overall IT Security Program Major Information System*, highlighted that 17 major information systems contained 93 terminated user accounts that were not disabled or deleted

within the required time period. Of the 93 user accounts not terminated in a timely manner, 42 were still active at the time of the audit.

- September 21, 2011 – OIG's report, *Significant Deficiencies Persist in DOL's Information Security Program*, noted that during access control testing, prior to the agency and OIG agreeing to stop escalation of privileges, OIG auditors reached a point where they could have obtained unauthorized, administrative system-level access to production systems containing PII.

- March 19, 2012 – OIG's report, *Federal Information Security Management Act Departmental Security Issues*, stated that OIG determined 95 separated employees retained access to network accounts after their departure for 9 of the information systems tested.

- March 31, 2015 – OIG's report, *Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information System*, showed separated user accounts were not removed in a timely manner. The report also stated users were granted privileged access without proper supervisory approval and rules of behavior acceptance, and a disabled account had been accessed inappropriately 52 days after the account end date.

Third-Party Oversight

Third-party oversight, which is oversight of parties that either own and operate systems on behalf of DOL or operate DOL-owned systems, has been cited as an issue in 8 of 11 Semiannual Reports that OIG issued to Congress over the past 5 years. These deficiencies included: physical and logical access controls not in place, improper use of shared accounts, system security assessments not performed, business impact assessments not performed, untested contingency plan, interconnections not fully documented, and agreements not in place. The following OIG Federal Information Security Management Act (FISMA) audits have identified a persistent pattern of third-party oversight deficiencies:

- March 30, 2010 – OIG's report, *Actions Required to Resolve Significant Deficiencies and Improve DOL's Overall IT Security Program Major Information System*, highlighted that DOL had not designed specific testing and monitoring policies or procedures for use by DOL system owners, Designated Approval Authorities, or contracting staff. These policies and procedures are needed to ensure compliance with minimum IT security requirements by third-party organizations operating or managing DOL IT systems.

- September 21, 2011 – OIG's report, *Significant Deficiencies Persist in DOL's Information Security Program*, noted the magnitude of third-party

oversight findings and the severity of their potential harm to systems, information, services, facilities, and people, required immediate actions by management to strengthen oversight of third-party providers and related systems.

- September 27, 2012 – OIG's report, *Department's Information Technology Security Program Is Weakened by Deficiencies*, found 21 control deficiencies within a third-party operated system. These deficiencies included: lack of physical and logical access controls, improper use of shared accounts, not performing system security assessments, not performing business impact assessments, not testing the contingency plan, not fully documenting interconnections, and not having agreements in place for interconnections.

- March 29, 2013 – OIG's report, *Department's Information Technology Security Program Is Weakened by Deficiencies*, emphasized DOL lacked specific policies and procedures to ensure adequate oversight of third parties that either owned and/or operated systems on behalf of DOL or operated DOL-owned systems. OIG's testing of two contractor systems identified substantial and pervasive risks to the confidentiality, integrity, and availability of mission critical and sensitive data.

- March 31, 2015 – OIG's report, *Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information Systems*, again found concerns with third-party systems. The report identified three major information systems operated on behalf of DOL with controls that were not operating as intended, as well as an overall lack of monitoring of the third-party service providers in two of those major information systems.

Inadequate third-party oversight also caused deficiencies in other control families, such as configuration management, incident response, background investigations, certification, accreditation, and segregation of duties. Government personnel oversight for contracted system services is required to maintain effective IT security controls. The lack of this oversight may cause specific security controls to remain unimplemented or ineffective.

Configuration Management

Configuration management has been reported as a recurring issue in the Semiannual Report to Congress four times over the past five years. The National Institute of Standards and Technology's Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* describes configuration management as a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems by controlling the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

- March 31, 2015 – OIG report titled, *Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information System*, found DOL lacked a process for the timely and secure installation of software patches and remediation of configuration-related vulnerabilities. Out of 20 specific deficiencies identified in the audit, 7 were within the configuration management control family.

Maintaining proper configuration management ensures integrity of information systems through a process for timely and secure installation of software patches and remediation of configuration related vulnerabilities.

Conclusion

We recognize DOL has developed Plans of Action and Milestones intended to remediate known information security vulnerabilities, and has completed numerous actions. Most recently, the United States Chief Information Officer instructed DOL and other federal agencies to immediately take a number of steps to protect federal information and assets and to improve the resilience of federal networks. As part of this effort, DOL is now working to implement multi-factor authentication for all DOL systems. However, we remain concerned that despite the reported progress in taking corrective actions, our audits continue to identify similar deficiencies in information security. Moving forward DOL needs to focus its efforts on enhancing its information security program to ensure the confidentiality, integrity, and availability of its information systems and data.

Recommendations

To further improve its information security program, we recommend DOL's Chief Information Officer: (1) place a focus similar to the PIV card implementation on implementing corrective actions related to the areas of significant deficiencies where we have repeatedly identified weaknesses; and (2) take a proactive approach in assessing security controls and correcting identified deficiencies across all DOL systems.

We request you respond to this memorandum within 10 business days. If you have any questions, please contact Keith Galayda, Director, Information Technology Audits at 202.693.5259.

cc: T. Michael Kerr
Ed Hugler
Tonya Manning
Nancy Rooney

U.S. Department of Labor

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

AUG 14 2015

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

FROM: DAWN M. LEAF
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2015 Audit Report entitled: Information Security Concerns, Report Number: 23-15-009-07-725

This memorandum responds to the above-referenced Fiscal Year 2015 audit report dated July 31, 2015. The Office of the Inspector General (OIG) summarized previously issued significant deficiencies in the areas of Access Control, Third Party Oversight and Configuration Management resulting in the issuance of two general recommendations.

The security of our information systems is one of the Department's highest priorities, and we are committed to ensuring that the Department implements safeguards to protect its systems and manage identified security risks. While DOL's pursuit of these remediation activities has been aggressive and unyielding, we will redouble efforts in accordance with the recommendations in your report.

Management acknowledges the perspective expressed in OIG's originally cited findings and articulates the same concerns stated in previous management responses. Previously, management has made the point that the audit reports do not provide the requisite linkage between the findings and risks or events that could be expected to rise to the level of seriousness contemplated by the term "significant deficiency," as defined by OMB.

Also relevant is the status of the OIG's prior recommendations reviewed in this report. In some instances, the OIG performed remediation testing and confirmed that corrective action had been completed for many of the outstanding weaknesses and closed out the associated recommendations. In other instances, the planned corrective actions are longer-term and are still in-progress. In these instances, the OIG has accepted these remediation plans as sufficient, with closure pending OIG verification.[1] In the interim, DOL's policies, procedures, and its physical and logically separated systems with supporting boundary controls collectively provide appropriate mitigating safeguards and redundant security measures.

[1] Attached is a crosswalk of the previous OIG reports referred to in the OIG's July 31, 2015 report cataloguing the status of the recommendations, as classified by OIG.

That being said, management appreciates the OIG's attention to information security. In particular, the [redacted] which is not the subject of this report, is an example of how the Department and the OIG can collaborate to improve information security. In that instance, management acted with urgency [redacted]

Management's response to the report's recommendations related to Access Control, Third Party Oversight and Configuration Management follows.

Access Control

Management concurs that Access Control is one of the most frequently cited and important aspects of recent OIG audit reports and agrees that this needs to be addressed. However, we have concerns with the completeness and accuracy of the subject report.[4] In some cases, several isolated access control related issues have been extrapolated from the various reports and combined with dissimilar issues to suggest a problem larger in scope than that is demonstrated by the analysis. Also, the statement: "DOL only recently began implementing this requirement in response to the Office of Personnel Management breach" does not acknowledge the fuller context of what the Department has done to improve access controls.

DOL had directed component Agencies to address system specific access control related issues well before the OPM breach occurred. For example, on August 14, 2012, DOL Agency Heads were briefed on the Departmental Risk Management strategy which highlighted the importance of addressing the identified deficiencies for access controls.

Following this briefing, on August 23, 2012, the Agencies' ISOs received Plan of Action and Milestones Training with a specific focus on addressing Departmental significant deficiencies. In parallel with these efforts, the Department initiated a comprehensive Enterprise Identity and Access Management (IAM) program to address systematic access control issues. This was communicated in previous management responses to the OIG and outlined in the DOL Plan of Actions and Milestones.

The Department's IAM Program, originally initiated in 2011, was re-planned in the spring of 2013 in part because a Federal Identity Credential and Access Management (FICAM) standard change rendered the selected product non-compliant. The project was re-initiated in November 2013 and officially chartered and approved by the DOL IT Project Review Board in FY 2014 Q2. The overall objective of the IAM program is to strengthen DOL's security posture by implementing an Identity Management (IdM) solution that will automate account management processes and enable user-based PIV Card authentication for all users to all DOL systems, including DOL cloud-based systems (e.g. Cloud email). Progress for DOL's Identity and Access

[redacted]

[4] Fiscal Year 2015 Audit Report entitled: Information Security Concerns, Report Number: 23-15-009-07-725.

Management program was impacted by Sequestration program budget cuts in late calendar 2013, FY 2014. However, despite funding reductions, in August 2014, DOL procured PKI Managed Services and successfully updated the DOL's Active Directory Infrastructure to support user-based PIV card logon functionality. Subsequent to the PKI implementation, DOL's FY 2015 IT Modernization budget was cut in the FY 2015 enacted budget, directly impacting the DOL IAM program funding.[5] In response, the project was re-baselined at a reduced level of effort focusing on the implementation of machine-based PIV Card logon for general users and user-based two-factor authentication for its privileged users.

By way of a September 7, 2014 Alert Memorandum, the OIG cited several significant security issues for the [redacted]. Although management, in its reply, noted several auditor misunderstandings about the [redacted] and the PIV card issuance process, management initiated an aggressive corrective action plan to address the identified deficiencies. The Corrective Action Plan called for the establishment of an Integrated Project Team that was chartered with responsibility to implement all required actions outlined in the Corrective Action Plan and to develop and implement a strategy that would enable DOL to leverage GSA's USAccess shared PIV services. The [redacted] IPT was able to complete corrective actions sufficient to close the majority of the identified weaknesses, and we have provided evidence to the OIG to verify closure of others. DOL also began leveraging GSA's USAccess shared PIV services and plans to be fully migrated within the next two years. Satisfied with management's actions, OIG classified the issue "resolved," with closure dependent on confirming completion of management's corrective action plans.

It is important to recognize that DOL-- both at the Departmental and Agency level -- has reallocated a tremendous amount of resources from other critical efforts to accelerate the program to support the Federal "CyberSecurity Sprint" targets. This effort has required technical and logistical assistance from OMB, OPM, and GSA, and diverted substantial resources, amounting to thousands of hours of staff time, to obtain the necessary credentials and equipment. Despite having no additional resources to undertake this project, the Department is proud that, as of August 14, 2015, we have implemented two-factor authentication for 78% of general users and 80% of privileged users. Additionally, DOL has developed a corrective action plan to ensure full compliance with two-factor authentication requirements by the end of FY 2015.

This too is deserving of context: Despite OMB's recommendation to increase DOL IT Modernization funding in FY 2015, the budget received from Congress cut the IT Modernization budget by $4.1M from the FY 2014 Enacted level and $15.4 from the Department's FY 2015 President's budget request. This lack of funding has directly impacted the ability of DOL to improve its IT security posture, including but not limited to the Identity Access Management project.

Finally, since the PIV two-factor authentication is only a sub-set of the scope of the IAM project, DOL will continue to implement additional Identity Management system objectives in FY 2016.

[5] It should be noted that the DOL funding constraint impacts on the IAM program were reported in the DOL FY 2014 Portfolio Stat and FY 2015 FedStat reviews.

Third Party Oversight

DOL, like other Federal agencies, faces technical constraints and challenges associated with the realities of the federal contracting process, service level agreements, and frequent cases where contractor proprietary system information limits the ability to physically verify security control implementation. However, the Department does apply standard security language and policies that clearly outline the contractor's responsibility to comply with all federal laws and mandates. Additionally, DOL's compliance review and oversight procedures include the review of DOL contracted systems. To ensure DOL agencies were positioned to address the unique challenges associated with performing security compliance reviews of third party systems, DOL developed and issued the DOL Third Party Security Monitoring Guide on May 11, 2015, and provided further implementation guidance on July 17, 2015. The Guide provides DOL Agencies and Information Security Officers with a uniform and consistent approach to complete oversight reviews and monitor third party/external information system providers. These reviews and associated results will be documented and jointly managed by System Owners and Information Security Officers.

Configuration Management

In reviewing the Department's configuration management control, the OIG has included topics outside the NIST defined scope of configuration management, in some cases even conflating configuration management with vulnerability management observations. That said, several of the OIG's observations are valid, and it is a top priority for management to resolve these issues promptly.

For example, DOL mitigated the impact of its budget constraints by becoming an early adopter of the Department of Homeland Security's Continuous Diagnostics and Mitigation program, and was able to enhance the DOL Information Security Continuous Monitoring (ISCM) program by adding more IT security monitoring tools. The DOL ISCM enables DOL to leverage automated tools for near-real time monitoring of DOL assets for vulnerability, configuration and asset inventory management. Further, the ISCM program provides agencies with the ability to automate many of configuration management procedures. As a result of implementing the ISCM program, DOL has experienced a significant decrease in the number of information system vulnerabilities, outstanding security patches, and configuration management shortcomings, indicating that the program is operating effectively. DOL's ISCM program will be further enhanced by the deployment of additional automated monitoring tools by the end of FY 2015.

To ensure that DOL addresses the remaining OIG configuration management issues and proactively strengthens DOL system configurations, the Department will continue the frequent ISCM security assessments and quarterly reporting process, including the issuance of quarterly security dashboards to monitor Agencies' progress in achieving the DOL security requirements. The Department will work with its Agencies to ensure effective corrective actions are identified to address any issues of concern. Corrective actions for all identified weaknesses are documented in the DOL Enterprise Plan of Action and Milestones, to which OIG access has been provided.

If you have any questions, please contact me directly at (202) 693-4200 or have your staff contact Tonya Manning, Chief Information Security Officer at manning.tonya@dol.gov or (202) 693-4431.

Attachment

cc: T. Michael Kerr, Assistant Secretary, OASAM
Ed Hugler, Deputy Assistant Secretary for Operations, OASAM
Tonya Manning, Chief Information Security Officer, OASAM
Keith Galayda, Director, Information Technology Audits, OIG

OIG IT Security Concerns Crosswalk

Report #	Report Name / Date	Recommendation	OIG Status	Source of Status
23-10-001-07-001 [OASAM has a copy of report]	Actions Required to Resolve Significant Deficiencies and Improve DOL's Overall IT Security Program Major Information System (March 30, 2010) *Two references in July 31 memorandum*	Recommendation 1: Develop an information security and risk-based assessment strategy resulting in identification of system security risks and priorities, and develop and link specific policies and procedures to those risks and priorities – a roadmap – for component agencies to follow in fully implementing minimum IT security requirements. Recommendation 2: Target areas of greatest risk for focused oversight and timely remediation of identified IT security program deficiencies. Recommendation 3: Develop and implement monitoring policies and procedures for component agencies to follow in the oversight of third-party compliance with minimum IT security requirements.	Recommendation 1 – Closed, pending OIG verification Recommendation 2 – Closed, pending OIG verification Recommendation 3 – Closed	Recommendation 1 – Memorandum from Elliot Lewis to Michael Kerr – *Updated Status of Prior-Year Recommendations Related to Chief Information Office IT Security* (July 18, 2011) Recommendation 2 – Memorandum from Elliot Lewis to Michael Kerr – *Updated Status of Prior-Year Recommendations Related to Chief Information Office IT Security* (July 18, 2011) Recommendation 3 - *Report No. 23-13-001-07-720: Verification of Office of the Chief Information Officer Remediation Efforts of Prior-Year Information Technology Security Recommendations* (October 4, 2012)
23-11-005-07-001 [OASAM has a copy of report]	Significant Deficiencies Persist in DOL's Information Security Program (September 21, 2011) *Two references in July 31*	Recommendation 1: Ensure appropriate resources are available to provide effective oversight and resolution of recommendations, including the timely remediation of all other identified IT security deficiencies.	Recommendation 1 – Resolved Recommendation 2 – Resolved	Recommendation 1 – Memorandum from Elliot Lewis to Michael Kerr – *Status of Recommendations for Fiscal year 2010 Audit Report Titled: Significant Deficiencies Persist in*

OIG IT Security Concerns Crosswalk

Report #	Report Name / Date	Recommendation	OIG Status	Source of Status
	memorandum	Recommendation 2: Assess the delay in implementing the Risk Management Compliance Program to ensure it is rolled out timely as an effective tool to assist in managing the IT security program.		*DOL's Information Security Program* (February 8, 2012) Recommendation 2 - *Report No. 23-13-001-07-720: Verification of Office of the Chief Information Officer Remediation Efforts of Prior-Year Information Technology Security Recommendations* (October 4, 2012) & Memorandum from Elliot Lewis to Michael Kerr – *Verification of OCIO Remediation Efforts for Prior-Year Information Technology Security Recommendations, Report # 23-14-001-07-725* (March 31, 2014)
23-12-002-07-001 [OASAM has a copy of report]	Federal Information Security Management Act Departmental Security Issues (March 19, 2012)	Recommendation 1: For the significant deficiencies, create a Plan of Action and Milestones with the highest priority in describing and implementing mitigation strategies and describe corrective actions having aggressive (immediate or near-immediate) milestone dates for correcting the three significant deficiencies access controls, background investigations, and oversight of third party systems to	Recommendation 1 – Resolved Recommendation 2- Resolved	Recommendation 1 – Memorandum from Elliot Lewis to Michael Kerr – *Verification of OCIO Remediation Efforts for Prior-Year Information Technology Security Recommendations, Report # 23-14-001-07-725* (March 31, 2014) Recommendation 2-

OIG IT Security Concerns Crosswalk

Report #	Report Name / Date	Recommendation	OIG Status	Source of Status
		ensure integrity, confidentiality and availability of information. Recommendation 2: For the other deficiencies, created a POA&M for describing and implementing mitigation strategies and describe corrective actions having milestone dates for correcting the three deficiencies: risk management, continuous monitoring, and contingency planning to ensure integrity, confidentiality and availability of information.		Memorandum from Elliot Lewis to Michael Kerr – *Verification of OCIO Remediation Efforts for Prior-Year Information Technology Security Recommendations, Report # 23-14-001-07-725* (March 31, 2014)
23-12-009-07-001 [OASAM has response to OIG]	DOL Needs to Take Immediate Action to Correct Security Weaknesses in the [redacted] (September 7, 2012)	Recommendation 1: Establish a prioritized corrective action plan, including milestones, detailing within 5 days that a detailed strategy to reduce or eliminate the related risks. Recommendation 2: Ensure system owners receive the training they need to meet their responsibilities.	Recommendation 1 – Resolved Recommendation 2- Resolved	Memorandum from Elliot Lewis to Michael Kerr – *Resolution Status of Information Technology Recommendations* (June 12, 2013)
23-12-007-07-001 [OASAM has copy of response to OIG]	Department's Information Technology Security Program is Weakened by Deficiencies (September 27, 2012)	Recommendation 1: Lead prioritization of agencies' remediation of the significant deficiencies identified by completing implementation of its planned, risk-based management and compliance program DOL-wide.	Recommendation 1 – Closed, pending OIG verification	Memorandum from Elliot Lewis to Michael Kerr – *Resolution Status of Information Technology Recommendations* (June 12, 2013)
23-13-008-07-001 [OASAM has a copy of report]	Department's Information Technology Security Program is Weakened by Deficiencies (March 29,	Recommendation: Reassess and establish DOL agencies' remediation priorities of the identified significant deficiencies to minimize risks to	Recommendation 1 – Closed, pending OIG verification	August 14, 2015 email from Elliot Lewis to Ed Hugler

OIG IT Security Concerns Crosswalk

Report #	Report Name / Date	Recommendation	OIG Status	Source of Status
	2013) *Two references in July 31 memorandum*	confidentiality, integrity, and availability of information and information systems. Note: Recommendation cites 23-12-009-07-001 (above)		
23-15-001-07-725 [OASAM has a copy of report]	Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information System (March 31, 2015) *Three references in July 31 memorandum*	Recommendation 1: Establish third-party oversight/monitoring processes and tools that guide information system owners on how to better monitor third-party service providers' effectiveness in implementing NIST information security requirements and Administration priorities. Recommendation 2: Increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to the Vulnerability and Configuration Management Significant Deficiency. Recommendation 3: Increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Contingency Planning / Disaster Recovery. Recommendation 4: Increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Access Management.	Pending formal response from OIG to management's response of March 27, 2015 to draft report	August 14, 2015 email from Elliot Lewis to Ed Hugler

OIG IT Security Concerns Crosswalk

Report #	Report Name / Date	Recommendation	OIG Status	Source of Status
		Recommendation 5: Conduct better oversight of DOL's information technology asset and incident response management areas to prevent unauthorized and unmanaged devices from handling DOL information and to ensure all incidents are timely reported to CSIRC and US-CERT.		