BULLETPROOF

a GLI company

OSL SR13398 BIENNIAL SECURITY REVIEW 2020 PUBLIC REPORT

FOR

OREGON STATE LOTTERY

Bulletproof Solutions
11 Ocean Limited Way, Suite 130
Moncton, NB, E1C 0H1

SN20097

Document Details	
Client	Oregon State Lottery
Locations	500 Airport Rd SE, Salem, OR 97301
Title	Biennial Security Assessment
Author	Scott Finck
Bulletproof Tester(s)	Scott Finck, Senior Consultant Thomas Bierbach, Senior Manager Rizwan Ahmed, Senior Engineer Scott Melnick, Practice Lead John Tuyen, Security Consultant
Reviewed By	Phillip Young
Approved By	Alisa McRae
Classification	Public

Key Dates	
Assessment Start Date	September 8, 2020
Assessment Completion Date	December 1, 2020
Draft Report Issue Date	December 16, 2020
Final Report Issue Date	February 18, 2021

Distribution List
Mike Wells, Assistant Director of Security John McKean, Supervisor Technology Risk and Compliance Kerry Figgins, Manager, Security Ken Magnus, Manager, Cybercrime

Table of Contents

Executive Summary

The purpose of this engagement was for Bulletproof Solutions Inc.(Bulletproof) to conduct a biennial security assessment for Oregon State Lottery (hereafter, "OSL"). This assessment included the following sections as outlined in work order contract #13398 "For Biennial Security Review Services" dated July 15, 2020, in accordance with the requirements of Oregon Revised Statute 461.180(6) ("Security Review") and as described in the contracted Statement of Work.

The report deliverable from this review represents an assessment of the current state of security of OSL's lottery operations, evaluating the adequacy of the controls or identifying risks and offering recommendations for possible improvements.

About Bulletproof

Bulletproof has been regularly and continuously engaged in the business of providing services performed by our Information Technology professionals. In fact, for nearly 20 years, Bulletproof has focused on helping clients navigate the increasingly complicated security landscape. Our highly qualified experts have performed approximately 225 security risk assessments for gaming and lottery clients. We have completed security reviews for numerous lottery industry organizations, including the Multi-State Lottery Association (MUSL), North Carolina Education Lottery (NCEL), the Florida Lottery, Missouri Lottery, Virginia Lottery, and the Wisconsin Lottery that were similar in scope to those activities performed in Oregon.

Review Scope

Utilizing industry best practices to perform a comprehensive study and evaluation of all aspects of security of Oregon State Lottery operations, the scope focuses on both internal and external threats to the Lottery's overall security as defined in ORS 461.180. Bulletproof reviewed and assessed the Lottery's technology infrastructure, security environment, and security systems by gathering information through surveys, documentation review, walkthroughs, network and systems review, and interviews with Lottery staff and management. Bulletproof used the results of its findings to identify security risks or issues and recommend short term and long-term corrective or mitigative actions.

Assessment Conclusion

Bulletproof has completed the Biennial Security Assessment for 2020 in accordance with defined scope of work. The assessment broadly reviewed security across operations at OSL. As the scope of the assessment was large, it is convenient to summarize results across specific domains. The results of the assessment can be summarized in five partial domains:

- Core lottery operations
- VLT lottery operations
- NIST 800-53 and IT security controls
- Threat Assessment and Scenario Based Testing
- Azure Security Posture

Core lottery operations

In reviewing the partial scope of the core lottery operational processes, Bulletproof has found a robust security framework and control environment, well documented policies and procedures, dedicated and experienced staff, and a culture of continuous improvement.

While it is virtually impossible to eliminate all security risks or risks of errors in lottery operations and gaming systems in general for as long as humans are involved in the process and interact with technology, security and integrity risks can be mitigated to reduce the likelihood and impact of a risk event to acceptable levels.

In summary, OSL's overall operational processes, and its policies and procedures meet the relevant control standards as well as current global industry best practices. The result of this review of the current state of the lottery operations security controls at OSL confirms a well-designed, well-established security management framework and mature processes.

VLT lottery operations

Bulletproof's assessment of lottery VLT operations shows that OSL's VLT lottery security is built upon a well-organized and thorough practice of rigorous testing and monitoring of VLT's adherence to the industry's leading standards.

OSL implements a multi-stage testing process with controls in place at every step of VLT development, implementation, and operation. From the initial contracting of vendors to the testing and certification of VLT hardware and software by an independent test laboratory to operational security in monitoring and change management, OSL has demonstrated mature controlled processes to secure VLTs at all stages.

As a GLI company, Bulletproof has unique insight into OSL's VLT security posture in comparison to other regulated jurisdictions. On the whole Bulletproof finds that OSL's VLT operational practices meet or exceed the standards of the industry for testing and assuring the legitimate operation of VLTs.

NIST 800-53 and IT security controls

With minor exceptions noted in the findings of this report, OSL maintains a mature information security program across information technologies systems in its control. In assessing the maturity of specific categories of controls to the NIST Cybersecurity framework few areas showed significant gaps in control maturity while many others are well defined and effective.

Where gaps do exist, the interviewed staff proved knowledgeable of the actions needed to close the gaps and, in several cases, described plans for future action that have already been determined.

The NIST Cybersecurity Framework is designed around practical approaches to improving maturity of security controls. NIST CSF includes stages of categories that build upon foundations. Gaps that exist in the foundational categories of controls propagate to other categories and can have far reaching effects. For this reason, it is worth noting that the few findings in the NIST CSF assessment are related to control categories in the foundational core stage of Identify and represent early priorities necessary for effectively managing security. While the overall IT security posture of OSL is relatively mature it can be beneficial to address the findings to better allow all controls to be managed for improvement.

Threat Assessment and Scenario Based testing

As part of this Biennial assessment technical testing was focused into specific areas of threats that were deemed reasonable to test. This approach allowed for precise planning and execution of test scenarios designed to identify and document specific risks. Testing was enacted and completed according to planned threat test scenarios and Bulletproof provided detailed analysis of results in a threat assessment report. While threats of low risk were identified, it is noteworthy that the majority of tested scenarios showed that theoretical risks could not be demonstrated in testing, a sign of effective security controls.

Azure Security Posture

In this Biennial assessment Bulletproof directed testing resources and expertise specifically to evaluate OSL's security posture in the Azure cloud environment. This is an area in which OSL has begun a process of change as systems are migrated into cloud based Azure resources. Given the early stage in this migration process the scope of Azure

resources used by OSL is subject to significant change going forward. Bulletproof's assessment has reviewed the full scope of all available resources. As should be expected in this case the results of Bulletproof's assessment identify a number of areas for improvement, many of which are not applicable to OSL's current resource deployment. Technical configuration gaps have been detailed to OSL in an Azure Security Posture report but should be best utilized in conjunction with analysis of security configurations for utilized production resources and resources being brought into the live production environment. By reviewing new resources for security configuration prior to deployment and against the configuration recommendations documented in the report OSL should be able to stay on top of its Azure security posture and show continued improvement going forward.

Assessment Conclusion

At conclusion of this engagement the results of the assessment demonstrate that the general security at the Oregon Lottery is well defined and effective. Overall, the security posture of the Lottery is positive, with relatively few areas of risk and effective controls protecting the confidentiality, integrity, and availability of the data. In both lottery specific focus areas and IT security controls, the Lottery is above average compared to other lotteries we have recently tested and industry peers in the gaming sector. This is a similar conclusion to previous biennial assessment reviews.

As a result of this engagement Bulletproof has noted eight findings of risk in the assessed areas, a number similar in degree to previous assessments. In all cases Bulletproof has classified the assessed risk levels as low. Bulletproof recommends continued vigilance in security by addressing the low-risk findings according to OSL's available resources and ease of remediation.

Summary of Findings

The following table outlines a summary of findings resulting from the review:

ID	Finding	Risk
	2.2 Lottery Game Retailer Security	
1	Retailer background check investigation not conducted regularly	**Low**
	2.13 Security Involving Unclaimed Prizes	
2	Gap in audit trails for identifying unusual patterns of late payouts	**Low**
	2.21 NIST 800-53 Control Assessment	
3	OSL lacks a mature asset management solution	**Low**
	2.21 NIST 800-53 Control Assessment	
4	OSL can improve IT asset risk management by defining clear definitions for priorities, constraints and risk tolerance in alignment with organizational risk strategy.	**Low**
	2.23 Threat Assessment and Scenario Based Testing	
5	Obsolete algorithms observed in VLT network communication configuration	**Low**
	2.23 Threat Assessment and Scenario Based Testing	
6	Database encryption key change procedures are not standardized	**Low**
	2.23 Threat Assessment and Scenario Based Testing	
7	Confidential documents are emailed as attachments	**Low**
	2.24 Azure Security Posture	
8	Azure security hardening process gap	**Low**

Table 1: Summary of Findings

Background

Review Approach and Methodology

To fulfil the requirements of this review, Bulletproof has taken the following approach:

- Bulletproof managed the selected scope and requirements above by grouping them logically and mapping them back to the various security control domains as described within industry best practices and standards.
- The team utilized a standard risk-based review methodology for this engagement, which contained four phases: planning, assessment, analysis, and reporting, which delivers a purposeful, quality product.

Following this approach, Bulletproof conducted the review in four phases.

Phase 1 – Planning

Bulletproof's planning for the security review included the following steps:

1. Development of working papers, checklists, and review protocols, mapping and base-lining relevant control references.
2. Planning of fieldwork review together with OSL. We established project timelines, assigned resources, identified key, and developed an initial schedule of interviews and meetings.

Phase 2 – Remote Assessment

Bulletproof conducted a process-based remote assessment, which began with a desktop review of all operational policies and procedures. This review allowed our team to assess the organizational security structure along with the established electronic draw system management processes. The review has been conducted remotely utilizing collaborative document sharing and videoconferencing technology under previously established guidelines and protocols.

The objectives of this stage were to:

- Review OSL's security management framework.
- Collect necessary information for optimizing the review to focus on critical risk areas.
- Consider the key variables of technology, people, and process.

This review included interviews with key lottery as well as vendor personnel, and review of critical documentation and records.

The assessment phase included the following steps:

1. Document review

   Bulletproof performed a review of critical documents and records with the following objectives:

   - General understanding of the workings of the OSL security management framework.
   - Review documented policies and objectives.
   - Review documentation of controls and procedures.

2. Identification of specific processes and interviews with process owners which provided the opportunity to:

   - Assess OSL's specific conditions and controls.
   - Meet lottery personnel and validate responsibilities.
   - Assess policies and procedures and security controls.

- Conduct general observations of security management operations.

Phase 3 – Analysis

Bulletproof analysed the results obtained during the assessment phase in order to provide an assessment of the state and maturity of OSL's security operations and to identify risks and recommendations for improvement, if any.

a. Completed analysis of findings

    - Where necessary, Bulletproof completed further investigation of the findings from the assessment phase and validated the risk analysis of the findings.

b. Developed results and recommendations for improvement

    - Based on any findings, Bulletproof developed security control recommendations to mitigate the risks identified in the review.

Phase 4 – Reporting

Bulletproof's reporting phase includes the following steps:

1. Develop a draft report.
2. Client review of the draft report.
3. Complete and submit the final report.

Observation Detail

Personnel Security

OSL maintains controlled processes to address the evaluated areas of personnel security according to the requirements of the organization. Policies and procedures for recruiting, hiring practices, and personnel are well documented. An organizational chart is maintained and kept current. Employees systematically acknowledge acceptance of personnel policies. A mature talent management process is in place and controlled with an electronic system secured with logical access controls that limit access rights on a need-to-know basis. A controlled training and security awareness program is implemented for all employees.

The review team has identified no findings in this scope section.

Lottery Game Retailer Security

OSL retailers are engaged under three different contracts specific to traditional lottery retailer, video lottery retailers, or a combination of the two. All policies and procedures for the management of the OSL retailer network are well documented and security requirements are defined. Administrative rules lay out the security requirements in descriptive form for all retailers within the Oregon State Laws and Oregon Revised Rules (OSR) as well as Oregon Administrative Rules (OAR). The retailer application and selection process is comprehensive and applies layers of checks and balances as well as requirements to ensure the suitability of every retailer applicant prior to engaging in a contract.

Bulletproof has identified one finding in this scope section:

Finding # 1: Retailer background check investigation not conducted regularly. Control: 2.2 Lottery Game Retailer Security - e. Background Investigation Process for Retailers Objective: To ensure up to date background check information on OSL retailers.	
Risk Level	**Low**
Finding(s):	
OSL has a retailer background check policy and procedure by which all retailers are required to undergo a background check prior to approval of their retailer application. The background check is not conducted regularly or periodically thereafter. OSL has already launched a project to expand the background check process to require periodic re-checks of retailers.	
Recommendations:	
OSL should pursue the implementation of regular background investigations on its entire retailer base. While this can be operationally onerous, a risk-based approach could be implemented which prioritizes retailers based on previous investigations or disclosures.	

Lottery Contractor Security

OSL Lottery and Contractor procurement contracts are conducted according to the requirements of ORS 461.410 and classified according to the requirements of OAR 177-037-0020. A controlled process for classifying contracts according to the required classification sensitivity levels of Major, Sensitive, or General is initiated by personnel responsible for procurement.

Contracts are managed through the procurement process by daily activities of Procurement personnel. Compliance with procedures is subject to audit by a lottery audit team that may choose to validate the standard processes. Background check processes are in place for Security personnel to review vendor suitability.

The review team has identified no findings in this scope section.

Security of Manufacturing Operations of Lottery Contractors

Lottery Contractor Manufacturing operations are subject to multiple stages of security control processes to define security requirements and verify these requirements are met. Contracts may stipulate the laws that the vendor is required to meet and may require insurance coverage from the vendor. Vendors undergo background checks in the contract procurement process. Security of manufacturing operations of lottery contractors is maintained according to defined technical standards and within the industry guidelines and recommendations of the independent test laboratory.

The review team has identified no findings in this scope section.

Security against Ticket Counterfeiting and Alteration and other Means of Winning

OSL Product Management has developed, documented and implemented requirements, measures and controls for security against ticket counterfeiting and alteration and other means of winning in all its lottery products based on industry best practice. These measures cover a wide scope of security controls in the design of the instant tickets. The features are designed and implemented to enable detectability of tampering attempts with a ticket.

The review team has identified no findings in this scope section.

Security of Drawings Among Entries or Finalists

OSL has implemented comprehensive policies and procedures addressing the promotional drawings, the promotional program rules and procedures as they pertain to the individual promotions. The policies and procedures are well documented and categorized. OSL utilizes Electronic Draw Systems (EDS) to conduct raffle type draws, called promotions, from a population of eligible entries. OSL has established robust logical access management policies and procedures in the promotional drawing and EDS operation, including the controls for collecting and safeguarding entries.

The review team has identified no findings in this scope section.

Security in Distribution

OSL's ticket testing procedures and methodology are in line with industry best practices. The Distribution and Facilities Associate Manager manages the distribution center and warehouses, including mail delivery throughout the organization. In the case of a security irregularity, staff report to their supervisor and escalate to security about the incident for incident response procedures and investigation.

The review team has identified no findings in this scope section.

Security involving Validation and Payment Procedures

OSL maintains effective security in validation and payment procedures. The validation, claims, and payment of prizes at OSL are managed within the Player service department with the involvement of security specialists to ensure the integrity and security measures in the validation and payment procedures are maintained. The security specialist team further investigates fraudulent claims and the integrity of scratch ticket games. The department has implemented policies and procedures around the validation and payment process.

The review team has identified no findings in this scope section.

Security Unclaimed Prizes

OSL has a mature process with established procedures specifically related to the protection of unclaimed prize money and data files containing information relating to the payout status of each game, the specific transactions yet to be claimed and the validation files. The procedures cover the entire prize payout period as well as the auditing of the final transfers upon game settlement and the rules covering ticket validity time, payout on lost and defaced tickets, inquiries into the validity of claims and late or last-minute payouts.

Bulletproof identified the following finding in this scope section:

Finding # 2: Gap in audit trails for identifying unusual patterns of late payouts Control: WLA SCS:2016 L.4.2.9 -Audit trails & 2.13.h. Review audit trails for identifying unusual patterns of late payouts Objective: To secure unclaimed prize money before and after the end of the prize claim period.	
Risk Level:	**Low**
Finding(s):	
There is no active auditing to identify unusual patterns of late payouts.	
Recommendations:	
OSL should build on its exception claim process and existing system data to create an audit trail, such as a report, which specifically identifies online winning transactions nearing their expiry date and also audit late payouts of prizes to enable the identification of patterns of late payouts. The audit trail could identify specific games and prize levels for examination, such as high jackpot prizes where the risk in late payouts is elevated.	

Security Aspects Applicable to Each Particular Lottery Game (VLT focus)

OSL maintains a thorough process to test security for VLT games. Each new video lottery game is subject to multiple stages of security control processes to define security requirements and verify these requirements are met.

Video Lottery Terminal games are produced by approved contracted vendors. Vendors submit game software to an independent test laboratory for testing against documented technical standards. Only games that are fully tested and certified to meet standards are deployed to OSL's video lottery terminals. VLT games are additionally tested in a pre-production environment before deployment and are monitored for performance while in active production. OSL additionally maintains and performs a robust change management process over the video lottery central system.

The review team has identified no findings in this scope section.

Video Lottery Games (VLG)

OSL actively monitors and audits the integrity of video lottery games according to industry standard practices using tested mathematical and technical means to ensure that games pay and play as designed. Games are monitored in real time for anomalies, and game performance is audited to conform with theoretical mathematical payouts. Monitoring for game anomalies occurs at multiple levels. OSL maintains a staff of field technicians that respond to anomalies reported from players and retailers. A hotline is in place for reporting these anomalies and is continually monitored by OSL personnel. The video lottery central system also supports monitoring of real time events as reported by the VLTs.

The review team has identified no findings in this scope section.

Video Lottery Miscellaneous

OSL maintains thorough security controls for Video Lottery operations. VLT games enforce a technical control process for claims and payments. OSL's video lottery recruiting and approval process is standardized and subject to OSL's controlled procedures for personnel security. OSL monitors for counterfeit video lottery machines and usage of such machines is prevented by multiple controls.

The review team has identified no findings in this scope section.

Security of Drawings in Lottery Games Where Winners are determined by Drawings of Numbers

OSL operates the local, instate draw games Megabucks, Lucky Lines, Keno, Pick 4. The draws for these games are conducted automatically through the gaming system's electronic draw systems. The OSL Raffle, and Second Chance draws are conducted by OSL staff utilizing automated draw machines. OSL partakes in the multijurisdictional games of Mega Millions and Powerball and does not conduct the actual draws for these games, but does conduct the procedures prior and post draw, where the relevant controls apply equally.

OSL has chosen the WLA Security Control Standard SCS:2016 as guidance for the security of drawings in Lottery Games Where Winners are determined by Drawings of Numbers. Applicable WLA controls were assessed in this review.

The review team has no findings identified in this scope section.

The completeness of security against locating winners in Lottery games with preprinted winners by persons involved in their production, storage, distribution or sale

OSL provides secure processes to control risks related to identification and validation of winners of preprinted tickets. OSL has demonstrated processes to investigate situations where people attempted to tamper with the scratch tickets. Investigations have been adequately conducted. A reconstruction process can be invoked to identify ticket details and winning information during an investigation.

The review team has no findings identified in this scope section.

Physical Security

OSL maintains physical security to industry standards. Due to limitations on travel and physical visitation imposed by quarantine requirements during the 2020 pandemic physical activity on site at OSL locations was limited to specific activities supported by local OSL staff. Bulletproof evaluated physical security based on confirmation with OSL staff of the physical security reviewed in prior assessments of OSL by Bulletproof, including past escorted walkthroughs of the lottery headquarters and the Wilsonville Claim Center. Physical security was additionally assessed in policy and procedure review and in interviews with staff. Based on the assessment Bulletproof reaffirms that Physical and Environmental controls adequately meet security standards including those documented in NIST 800-53.

The review team has no findings identified in this scope section.

NIST 800-53 Control Assessment

Bulletproof has performed a comprehensive assessment of OSL's information security controls using the NIST Cybersecurity Framework (NIST CSF) and referencing related NIST 800-53 Control standards for specific control guidance. This review encompassed assessment of OSL's information security practices across multiple functions as defined by the NIST CSF.

In assessment of OSL's information technology security controls Bulletproof has evaluated control maturity according to the NIST CSF framework and reference the NIST 800-53 standard for specific guidance and control recommendations.

Bulletproof's assessment of OSL's security practices to the NIST CSF additionally covered other IT information security scope requirements of the Biennial Security Assessment. The assessment included computer security topics across NIST CSF categories. Bulletproof additionally assessed OSL's IT security practices for data communication security, wireless security, database security, application security, and the Lottery's Organizational Structure as it relates to Information and Network security through the process of the NIST CSF assessment.

The results of Bulletproof's assessment of OSL's NIST CSF maturity were detailed and reported to OSL. The assessment team has noted two findings relating to evaluated NIST CSF controls. Outside of these findings our assessment indicates a relatively robust and mature security posture, although there is still room for improvement.

Bulletproof identified the following two findings in this scope section:

Finding # 3: OSL lacks a mature asset management solution Control: NIST CSF ID.AM-1; ID.AM-2; ID.AM-4; ID.AM-5 Objective: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
Risk Level	**Low**
Finding(s):	
It was identified that OSL does not have a well-defined asset management solution in place to organizationally, centrally, and systemically identify and track assets. Subject matter experts at OSL are aware of this gap and have noted that plans are in place to obtain and implement an asset management solution in the future.	
Recommendations:	
OSL should determine and implement an asset management system to standardize tracking of assets across the organization. Assets should then be secured according to organizational objectives and risk strategy.	
Finding # 4: OSL can improve IT asset risk management by defining clear definitions for priorities, constraints and risk tolerance in alignment with organizational risk strategy. Control: NIST CSF ID.RA-4; ID.RM-2; ID-RM-3 Objective: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
Risk Level	**Low**
Finding(s):	
Information technology (IT) asset risk assessment should be guided by clear and standardized criteria for organizational priorities and risk tolerances. Currently OSL does not define clear criteria at the level of IT risk assessment, although OSL does maintain a mature organizational risk strategy. A formalized approach to evaluate IT asset risk in accordance with existing risk strategy with clear expression of organizational risk tolerance and critical infrastructure is necessary for alignment of IT asset risk decisions with existing organizational risk strategy and processes. Assets deemed critical to the organization should be determined according to standardized criteria such that risk decisions are agreed upon and prioritized the same throughout the organization. Risk determination criteria for IT risk assessment should follow and/or align with organizational risk strategy such that IT risk assessment has clear definitions of critical assets and risk levels that support organizational risk decisions.	
Recommendations:	
OSL should standardize risk assessment criteria for assets in alignment with risk strategy at an organizational level, with clear priorities and risk levels and tolerances formally agreed with or established by the organization.	

Threat Assessment and Scenario based testing

Bulletproof has conducted a scenario-based threat assessment and testing in accordance with the biennial assessment scope. In the course of the biennial security assessment Bulletproof interviewed subject matter experts in a holistic multi-discipline review of security. As a result of these interviews and based on Bulletproofs expertise in lottery and security industries, Bulletproof security assessors identified a series of potential threats. The threats were identified with the objective of determining specific testable scenarios for which risk could be analyzable and potentially demonstrated as realizable. After an initial exercise identifying threats, the Bulletproof assessment team discussed the practicality and usefulness of performing tests with the OSL security management team. As a result of this discussion, specific test scenarios were marked for testing and Bulletproof coordinated with OSL for execution of the selected test scenarios. Risks were identified and analyzed for any tested in which a realizable risk was demonstrated. Technical findings with recommendations have been provided to OSL.

Bulletproof identified the following three findings in this scope section:

Finding #5: Obsolete algorithms observed in VLT network communication configuration	
Risk Level	**Low**
Finding(s):	
A theoretical weakness was observed in the communication configuration of the VLT test network. The observed server certificate is signed using a SHA-1 algorithm, which is considered less secure than newer algorithms.	
Recommendations:	
Industry standards, including NIST, recommend obsoletion of SHA-1 algorithms in favor of more secure algorithms such as SHA-2. The current risk is low, but it is recommended that future VLT certificate issuance software or processes be migrated to use certificates with SHA-2 algorithms.	
Finding #6: Database encryption key change procedures are not standardized	
Risk Level	**Low**
Finding(s):	
The procedures used by database analysts when changing encryption keys for encrypted fields in OSL managed databases are not organized, documented or tested.	
Implications:	
Recommendations:	
It is recommended that the data fields and keys required for encryption changes be identified and documented, along with the procedures and references used in the past operations for encryption. A standardized, controlled and tested process for changing encryption keys is a recommended step in order to be prepared to respond to certain security incidents.	

Finding # 7: Confidential documents are emailed as attachments	
Risk Level	**Low**
Finding(s):	
A process was identified in which confidential documents are emailed from OSL to vendors as standard email attachments that are at risk of exposure to third parties. Current processes in interactions between OSL Procurement team members and Vendors include exchanging contract document drafts as standard email attachments.	
Recommendations:	
Remediation of this risk is of low cost and effort and is therefore recommended. Technical solutions exist to communicate documents with secure links rather than directly as email attachments. It is recommended that training on these solutions be provided to the Procurement team and to anyone in the organization that may email confidential information or email attachments to external parties.	

Azure Security Posture

Bulletproof has assessed OSL's Azure Security Posture In accordance with the scope of this biennial security assessment Bulletproof specialists in Azure security have reviewed OSL's Azure security posture in order to identify weaknesses and take further action on recommendations to strengthen their cloud security. This assessment focused on the current state of the Azure tenant, recommendations for the future security state, and high-level remediation plans. Remediation recommendations focus upon technical configuration settings that can be changed to align with industry best practices, including settings that will provide demonstrable technical controls for security compliance standards.

Bulletproof assessed the full domain of OSL Azure resources against security controls to provide a baseline of the current configuration, and Bulletproof has made specific technical recommendations. The results of the assessment were provided in technical detail to OSL. While the full list of technical recommendations is provided in that report, the results of the assessment are therefore summarized in a single finding as shown below.

Bulletproof identified the following finding in this scope section:

Finding # 8: Azure security hardening process gap Objective: To improve OSL's Azure security process according to risk tolerance	
Risk Level	**Low**
Finding(s):	
Implications:	
As OSL migrates systems to the Azure resources security configurations should be reviewed and determined systematically. Without a standardized and controlled approach to security configuration hardening resources are subject to unnecessary security risk.	
Recommendations:	
OSL should assess Azure resources and planned Azure migration activities to determine which systems require configuration settings to be hardened. OSL should standardize security of deployed Azure resources and incorporate recommendations for technical configuration from Bulletproof's assessment.	

Terms and Conditions

All services provided by **Bulletproof Solutions Inc.** (the Contractor) to **Oregon State Lottery** (the Client) are provided in accordance with and subject to the Terms & Conditions as set forth in Oregon State Lottery Services Contract #13398 dated July 15th, 2020 and agreed to by both parties.