1. SYSTEM IDENTIFICATION

1.1. System Name/Title: TestGenius by Biddle Consulting Group, Inc.

1.1.1. System Categorization: Low Impact for Confidentiality. NIST SP800-171R2

1.2. RESPONSIBLE ORGANIZATION:

Name:	Biddle Consulting Group, Inc.
Address:	606 Sutter Street, Folsom, CA 95630
Phone:	916-294-4250

1.2.1. Information Owner (Internal stakeholder to your organization)

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (Internal security manager):

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. **System Security Officer,** (Security Assurance Staff Performing Assessment):

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.3. GENERAL DESCRIPTION/PURPOSE OF SYSTEM:

What is the function/purpose of the system? TestGenius is a skill and ability testing software (SAAS, cloud) that COD has been using for several years. COD is opting to use a version of TestGenius that is integrated with Workday.

1.3.1. Number of end users and privileged users:

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. GENERAL DESCRIPTION OF INFORMATION:

CUI information types processed, stored, or transmitted by the system are determined and documented. **First name, last name, and email address of job applicants who have been invited by our client to test**.

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices.

Provided as an attachment from trust site (Network Map, NDA is required. See trust site at https://community.testgenius.com/documents) to download NDA. Complete and email to support@biddle.com and they will return the network map to you by email.)

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component

Hardware	Hardware Uses	Comment
N/A		Cloud-based

2.2. List all software components installed on the system.

Software	Software Uses	Comment
TestGenius	Pre-employment applicant testing	https://online.testgenius.com

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **N/A Cloud-based subscription, no hardware.**

3. REQUIREMENTS

3.1. ACCESS CONTROL

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Access control is managed by client, who is able to set up and revoke user access and set permissions for each user. Access is managed by client solely.**

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Access controls by software function include: Validation, Test Selection Wizard, Test Battery Setup, Invitation Management, Test Link Status, Custom Tests, Reporting, Proctoring Reports, User Accounts Management, and Help sections.**

3.1.3. Control the flow of CUI in accordance with approved authorizations.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, the CUI is managed by function as per above, with the access managed by COD administrator(s).**

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Same as with 3.1.3, above.**

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, as per 3.1.3, above.**

3.1.6. Use non-privileged accounts or roles when accessing non-security functions.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, as managed by COD using the functions set forth above.**

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, implicit in user access control permissions system.**

3.1.8. Limit unsuccessful logon attempts.

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **This is on track to be added in Q4 of 2025.**

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, implicit in system is a user-based notification system. The scope of such will be increasing in**

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, the system resolves to login screen after two hours idle time.**

3.1.11. Terminate (automatically) a user session after a defined condition.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Terminate by manual log out and by time, two hours idle, are both implemented.**

3.1.12. Monitor and control remote access sessions.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We run a SIEM on the Google Cloud network.**

3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Remote access only granted through VPN, forcing encryption.**

3.1.14. Route remote access via managed access control points.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All connections must run through VPN to Google Cloud network.**

3.1.15. Authorize remote execution of privileged commands and remote access to security-relevant information.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We follow “least privileged” for all internal user accounts.**

3.1.16. Authorize wireless access prior to allowing such connections.

□ Implemented □ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **No wireless access for us to grant client in this case. System is accessed by browser only.**

3.1.17. Protect wireless access using authentication and encryption.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Use secure authentication and encryption on internal networks.**

3.1.18. Control connection of mobile devices.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Restrict mobile device from connecting to server network, as well, mobile access by applicants is restricted when tests are not appropriate for mobile access.**

3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Encrypted en route to device, and viewable only in encrypted form in device browser.**

3.1.20. Verify and control/limit connections to and use of external systems.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **TFA with Duo, limiting access.**

3.1.21. Limit use of organizational portable storage devices on external systems.

□ Implemented   ☒ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Updating policy to include this in 2025.**

3.1.22. Control CUI posted or processed on publicly accessible systems.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Encrypted in transit and at rest. Access to be granted by COD master admin.**

3.2. AWARENESS AND TRAINING

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We run quarterly security trainings through “KnowBe4”. Also, our security experts are subscribed to several security feeds such as CISA.**

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, per above.**

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☒ Implemented   □ Planned to be Implemented   □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, as per above.**

3.3. AUDIT AND ACCOUNTABILITY

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **We run a SIEM.**

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **We run a SIEM and have Microsoft logging turned on for each user account.**

3.3.3. Review and update logged events.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **We run reviews on logs and SIEM monthly or quarterly depending upon the system.**

3.3.4. Alert in the event of an audit logging process failure.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **We are alerted if any SIEM collector goes down.**

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **SIEM and logs are monitored in real time by MSP team.**

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **We have not been doing this, but can do so upon request.**

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All logs are using a time server (MS.) Users do not have the ability to change / update, except for the primary engineer admin.**

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **No users have access to delete or modify logs. Must be requested through MSP.**

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

3.4. AUDIT AND ACCOUNTABILITY

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **MSP manages the inventory of the organizational systems.**

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **This in place and managed by MSP.**

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All handled by MSP.**

3.4.4. Analyze the security impact of changes prior to implementation.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All users created with required access only.**

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **MSP manages with RMM tools on each machine.**

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale**. Same as above.**

3.4.9. Control and monitor user-installed software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Same as above.**

3.5. IDENTIFICATION AND AUTHENTICATION

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Users are authorized and logged.**

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All users must be authenticated in order to connect.**

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Company network and TestGenius network require MFA to access. TestGenius user interface does not require MFA.**

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **For company and TestGenius networks, yes. For TestGenius user interface, we do not require.**

3.5.5. Prevent reuse of identifiers for a defined period.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale**. Last five passwords cannot be reused.**

3.5.6. Disable identifiers after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale**. Same as 3.5.4, except we do not remove any COD users from the TestGenius admin. Management of said users is by COD main admin or by direct request from COD admin, we can assist.**

3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale**. Following NIST best practices for passwords.**

3.5.8. Prohibit password reuse for a specified number of generations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes, last five.**

3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.

☒ Implemented ☒ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **This feature exists and can be turned on by request.**

3.5.10. Store and transmit only cryptographically-protected passwords.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes.**

3.5.11. Obscure feedback of authentication information.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes.**

3.6. INCIDENT RESPONSE

3.6.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Following NIST standards.**

3.6.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Following NIST standards.**

3.6.3. Test the organizational incident response capability

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Annually.**

3.7. MAINTENANCE

3.7.1. Perform maintenance on organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Install all updates within 72 hours, unless we see a problem in staging. In that case, we will work to resolve before pushing to production.**

3.7.2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **MSP implements controls for all system maintenance.**

3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale**. All devices are wiped and certified as such by MSP.**

3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes.**

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Only MSP has access and MFA is required.**

3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We do not provide access to non-credentialed maintenance persons.**

3.8. MEDIA PROTECTION

3.8.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All data encrypted at rest and all physical data is stored in locked, secured areas.**

3.8.2. Limit access to CUI on system media to authorized users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Access is allowed to only authorized employees.**

3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, see above.**

3.8.4. Mark media with necessary CUI markings and distribution limitations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **TestGenius client data is not copied to distributable media.**

3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

3.8.7. Control the use of removable media on system components.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **No removable media is allowed into TestGenius network.**

3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **No removable media is allowed into TestGenius network.**

3.8.9. Protect the confidentiality of backup CUI at storage locations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All backups are securely stored by MSP in the cloud.**

3.9. PERSONNEL SECURITY

3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes.**

3.9.2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We have a structured off-boarding process that HR and MSP follow.**

3.10. PHYSICAL PROTECTION

3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale**. Physical office is locked, but the data is stored only in the cloud.**

3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Alarms and door locks are in place where needed.**

3.10.3. Escort visitors and monitor visitor activity.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **No visitors are allowed in sensitive areas, and are monitored elsewhere.**

3.10.4. Maintain audit logs of physical access.

□ Implemented □ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We do not maintain an audit log of who visits our office.**

3.10.5. Control and manage physical access devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes.**

3.10.6. Enforce safeguarding measures for CUI at alternate work sites.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **We have no alternate work sites.**

3.11. RISK ASSESSMENT

3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Annually by Omnistruct, a security firm. We also run compliance in Hypercomply for NIST.**

3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale**. Quarterly.**

3.11.3. Remediate vulnerabilities in accordance with risk assessments.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Remedy all high or severe vulnerabilities immediately.**

3.12. SECURITY ASSESSMENT

3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Annually.**

3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **With assistance from MSP and Omnistruct.**

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes, using Hypercomply.**

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Rely upon Omnistruct, security firm, to review annually.**

3.13. SYSTEM AND COMMUNICATIONS PROTECTION

3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All communication is kept internal to company network.**

3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, following best practices.**

3.13.3. Separate user functionality from system management functionality.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Only managed by MSP.**

3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, using SIEM.**

3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All internal networks are separated logically or physically from public available systems.**

3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Only allow HTTPS traffic for TestGenius.**

3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale**. Split tunneling is not enabled.**

3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **All CUI is encrypted in transit.**

3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Yes, timing out after two hours of inactivity.**

3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If “Not Applicable,” provide rationale. **Managed by MSP.**

3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes, Google Cloud uses FIPS 140-2 validated encryption module called BoringCrypto.**

3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **New devices all set up by MSP.**

3.13.13. Control and monitor the use of mobile code.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **No mobile code is allowed on TestGenius.**

3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes, MSP managed.**

3.13.15. Protect the authenticity of communications sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All are through approved channels.**

3.13.16. Protect the confidentiality of CUI at rest.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Google Cloud encrypts all data at rest and in transit.**

3.14. SYSTEM AND INFORMATION INTEGRITY

3.14.1. Identify, report, and correct system flaws in a timely manner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **MSP monitors and notifies.**

3.14.2. Provide protection from malicious code at designated locations within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All users running TrendMicro.**

3.14.3. Monitor system security alerts and advisories and take action in response.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **MSP monitors and notifies.**

3.14.4. Update malicious code protection mechanisms when new releases are available.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **All definitions are kept up to date in real time.**

3.14.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Scanned weekly and any transferred files are scanned in real time.**

3.14.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. SIEM as well as AV.

3.14.7. Identify unauthorized use of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. MSP notifies immediately if detected.

4.15. NATIONAL DEFENSE AUTHORIZATION ACT 2019 (NDAA ACT), SECTION 889 SUPPLY CHAIN PROHIBITION– MUST ASSESS

4.15.1. Do the system, equipment or services comply with the **NDAA Act 2019 Section 889 ?**

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. Yes, Google complies.

4.15.2. Does the contractor provide a compliance certificate attesting to compliance with the **NDAA Act 2019 Section 889 ?**

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. Through Google.

4.16. SOC 2 – SOC FOR SERVICE ORGANIZATION: TRUST SERVICES CRITERIA

4.16.1. Does the vendor provide the **"Report on Controls for SOC 2 Attestation" at a Service Organization",** Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes, through Google Cloud.**

4.17. PCI DSS SCOPE – PAYMENT CARD INDUSTRY DATA SECURITY STANDARD SCOPE

4.17.1. Does this project utilize credit card payment processing and / or systems in any part of this project.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **TestGenius does not store any payment information, though the server through Google Cloud does have PCI certification. Company payment information is stored securely in Quickbooks cloud.**

4.17.2. If this project utilizes credit card payment processing and / or systems in any part of this project, does affected vendor have **PCI DSS Attestation of Compliance (AOC).**

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **It does not utilize card processing.**

4.17.3. If this project utilizes credit card payment processing and / or systems in any part of this project, does affected vendor have a completed PCI DSS Self-Assessment Questionnaires (SAQs).

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

4.17.4. If this project utilizes credit card payment processing and / or systems in any part of this project, does affected vendor have a completed **PCI DSS Remediation Plans** for identified controls weaknesses.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

4.17.5. Will this project be deployed into the client's **Card Data Environment (CDE).**

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **This project is a website accessed through a browser only.**

4.17.6. Will this project be deployed into the Vendor hosted client **Card Data Environment (CDE).**

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Same as above.**

4.18.1. BITSIGHT – SECURITY POSTURE RISK RATING ASSESSMENT

4.18.2. Does the Project Vendor have a record in BITSIGHT.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale. **Yes.**

4.18.3. Does The Project Vendor have ADVERSE RISK SCORE ?
VENDOR BITSIGHT POSTURE RISK SCORE: 750

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale**. Yes.**

4.18.4. **LIST ALL ADVERSE RISKS** Elements From Bitsight: NONE.

VENDOR BITSIGHT POSTURE RISK SCORE: 750

Vendor Bitsight Risk Element		Risk Score	Comment
1	N/A		None noted.
2			

3			
4			
5			

CYBER LIABILITY BREACH RISK ESTIMATE

RISK IMPACTS (800-53 Control Name & Control Number)	CONTROL IMPACTS (FAIR Spreadsheet)		ESTIMATED COST (FAIR Spreadsheet)	COMMENTS (Descriptions of Weakness Identified)
	CVSS 3.1	STRENGTH		
EXAMPLE: ACCESS CONTROL 3.1.1	**LOW** **1.0** **LOW**	6.0	$1.5 M – $3.0M	System does not assign unique ID and account to each user. Generic accounts used that creates difficulties identifying who performed unauthorized action on the system
EXAMPLE: ACCESS CONTROL 3.1.2	**VERY LOW**	6.0	$1.5 M – $3.0M	Permissions for system actions are not restricted, allowing any user to perform unrestricted actions on the system and potentially compromising integrity of the system or data.
EXAMPLE: INCIDENT RESPONSE 3.6.1	**LOW**	8.0	$1.0 M – $3.0 M	No mention of an established operational incident-handling capability for organizational systems that

RISK IMPACTS (800-53 Control Name & Control Number)	CONTROL IMPACTS (FAIR Spreadsheet)		ESTIMATED COST (FAIR Spreadsheet)	COMMENTS (Descriptions of Weakness Identified)
	CVSS 3.1	STRENGTH		
				includes preparation, detection, analysis, containment, recovery, and user response activities.