System Security Plan (SSP)

Version 1.0

ARIA Group, Inc.
17395 Daimler Street
Irvina, CA 92614
United States of America
CAGE 37JU8

July 2025

Version Information

Version	Date	Summary of Changes	Approver
1.0	1 July 2025	Initial Release	

Change Log

This document resides on the ARIA Group SharePoint site, which is our document repository for versioning and change log tracking. If printed, the user is responsible for verifying the latest version.

Approval

Owner	Title	Date	Signature
	Security Officer		
Approved By	**Title**	**Date**	**Signature**
	Chief Executive Officer		

Table of Contents

REFERENCE LIST

The following is a list of document references that are controlled versions maintained on the ARIA Group SharePoint server.

DOCUMENT REFERENCES

ARIA Group Network Diagram
ARIA Group Business Information Systems Map v1.0 Rev June 2024
ARIA Group Information Security Policy
ARIA Group Approved and Installed Software Listing
ARIA Group Ports, Protocols and Services Matrix (PPSM)
ARIA Group STIGs & SCAP Results
ARIA Group Remote User Access Policy
ARIA Group Remote User (Telework) Policy and Procedure
ARIA Group Insider Threat Policy and Plan

1.0 SYSTEM IDENTIFICATION

1.1 System Name/Title: ARIA Group Enterprise Network

1.1.1 *System Categorization: Moderate Impact for Confidentiality*

1.1.2 *System Unique Identifier : ARIA Group Enterprise Network*

1.2 Responsible Organization:

Name:	
Address:	
Phone:	

Name:	
Address:	
Phone:	

1.2.1 ***Information Owner (****Government POC responsible for providing and/or receiving CUI)****:***

Name:	Department of Defense (Various Agencies/Organizations)
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1 **System Owner** (assignment of security responsibility)**:**

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

1.2.1.2 System Security Officer:

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

1.2.1.3 IT Service Provider:

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

1.2.1.4 Information Security Provider:

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

1.3 General Description/Purpose of System:

ARIA Group is an 100% Employee-Owned Business formed in 1999 with engineers, analysts, logisticians, technicians, and information technology specialists who provide professional and engineering support services to multiple Navy organizations and the Department of Homeland Security. ARIA Group is headquartered in Virginia Beach, VA, and is supported by their Information Technology (IT) provider IT IT Services (IT) and Information Security (IS) provider Inovo InfoSec, Inc. (Inovo).

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
Approx.	

1.4 General Description of Information:

The ARIA Group Enterprise Network handles various forms of US Government information, including Controlled Unclassified Information (CUI), due to the work being performed for various agencies and organizations under contract. Financial, Privacy, Proprietary Business Information and Tax information are resident on the systems due to normal course of business operations and activities which take place in support of the business operations. All CUI information is protected and encrypted to Federal Information Processing Standards (FIPS) 140-2 requirements while in-transit and at rest within the servers and user operating environments. FIPS 140-2 is a U.S. government computer security standard. CUI is categorized in accordance with the CUI Registry at https://www.archives.gov/cui/registry/category-list.

2.0 SYSTEM ENVIRONMENT

The ARIA Group Enterprise Network is physically located in the following locations: Irvina, California and TC,. The ARIA Group Enterprise Network is comprised of physical and virtualized servers, laptops, and workstations for the User Operating Environment. The ARIA Group Enterprise Network facilitates the administrative (time & accounting, file shares containing customer related data, user data, system design, Personally Identifiable Information (PII)/Human Resources (HR) data, and other CUI level data) and users' day-to-day computing activities within the organization.

The Network Diagrams are depicted in Appendix A to this Document.

2.1 Hardware and Software Listings

Hardware and Software Listings are stored in Microsoft 365 using EntraID and Intune. The database includes a listing of all hardware and software (system software and application software) components, including make/OEM, model, version, service packs, and person the asset is assigned to. IT maintains this database for ARIA Group.

2.2 List All Software Components Installed on the System

All software components installed on ARIA Group systems are documented in the ARIA Group Evaluated and Approved Product Listing (E/APL) and stored in the IT ConnectWise Agent Database as discussed in Section 2.1. This listing is updated semi-annually with cyber risk assessments being completed for unapproved software not found on the NIAP, DOD E/APL (APLITS), DISA E/APL or DHS E/APL.

2.3 Hardware and Software Maintenance and Ownership

ARIA Group IT maintains the ARIA Group Enterprise Network and licensures for all supporting software and hardware. Licenses are procured in accordance with the IT procurement process. Only IT Administrators have direct access to licenses and can allocate them based on a formal ticket request. All requests are made through the ARIA Group Aria Operating System (AOS) and approved by the Chief Technology Officer (CTO). Once the approval is obtained, IT receives and completes the request. Any changes in licensure will be documented as part of the Asset Management Policy for the company. Freeware and Shareware are evaluated prior to utilization and documented in Intune. ARIA Group's Hardware/Software listing is updated by IT on a monthly basis using an agent which is installed on each ARIA Group owned asset. All hardware and software will be evaluated for NIST, FIPS 140-2 and NIAP compliance prior to procurement to ensure secure supply chain practices are executed per NIST 800-161. ARIA Group's secure supply chain is audited at least annually.

3.0 REQUIREMENTS

(Note: The source of the requirements is National Institute of Standards and Technology (NIST) Special Publication 800-171, Rev. 2, dated 28 January 2021)

The protection of CUI resident in non-federal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. NIST 800-171 Rev. 2 provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in non-federal systems and organizations; when the non-federal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of non-federal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

3.1 Access Control

3.1.1 *Limit System Access*

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

System access is restricted to authorized technical personnel ARIA Group using a combination of unique USERIDS and shared accounts. No system account with processes acting on behalf of authorized users are in place, and devices are not managed by a centralized Identity and Access Management System (IAM).

3.1.2 *Limit System Access to the Types of Transactions*

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

System access will be but is not yet limited to only authorized functions and transactions as required by ARIA Group staff in order to accomplish assigned tasks and services in support of customer and Defense Industrial Base (DIB) contracts. Users will accomplish functions and transactions utilizing the least privilege possible. Local Administrative Privileges will not granted to standard users.

3.1.3 *Control the flow of CUI in Accordance with Approved Authorizations.*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

CUI will be controlled with customized, restricted Access Controls on files, share drives, databases, and objects based off "Need-To-Know" which prevents disclosure to unauthorized personnel. Users will provided training on handling and disposal of CUI through annual security awareness training. Teleworkers will be advised of their CUI responsibilities in a written Aria Information Security Policy.

3.1.4 *Separate the Duties of Individuals*

Separate the Duties of Individuals to Reduce the Risk of Malevolent Activity Without Collusion

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ARIA Group will separate the duties between System Administrators and users to ensure user accounts cannot execute administrative functions and administrator accounts are strictly reserved for administrative duties. Administrative access is retained by authorized ARIA Group System Administrators. Local user administrative access will be prohibited. To prevent collusion, ARIA Group will form an Information Security Committee that audits all administrative functions and activities monthly in the ARIA Group Monthly Risk Management Meeting (MRMM). Any detected anomalies or unauthorized privileges will be immediately investigated and revoked if needed.

3.1.5 *Employ the principle of least privilege.*

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The principle of least privilege will be incorporated during account creation to ensure privileged accounts are closely monitored especially when acting on behalf of a critical service. Those accounts will be documented, not used for day to day productivity, and regularly audited monthly during the ARIA Group MRMM. User accounts will have the minimum privileges required to accomplish taskings and provide contractual support.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Authorized ARIA Group IT System Administrators will utilize User level accounts for all non-security functions and only elevate to the Administrative Level when required. These functions will be audited and reviewed in accordance with ARIA Group Information Security Policies. Non-Security functions are defined as support services such as new laptop delivery and configuration with the user, troubleshooting activities (connectivity, user training on new applications and functionality) and/or hardware deployment or replacement.

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

ARIA Group non-privileged users will be prevented from executing privileged functions via the implementation of Intune Policies which are pushed out to the Enterprise that define a user's role, their level of access to directories, share drives or files/objects. System Administrators can modify the Intune policies only with approval from the ARIA Group Information Security Committee. These activities will be audited as part of the Monthly IT Risk Management procedure. Intune Policies will be updated as needed when an updated version of applicable Security Technical Implementation Guidance (STIG) is published, or when new operating systems are approved for use at ARIA Group.

3.1.8 *Limit unsuccessful logon attempts.*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Unsuccessful logon attempts will be set to be in compliance with the STIGs at 3 unsuccessful authentication attempts locking out a user with the policy being enforced via Intune policies and Conditional Access Policies (CAP) using Microsoft EntraID. The lockout period will be defined at 15 minutes and users who lock themselves out can wait the 15 minutes or contact IT to have their access restored.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Privacy and Security Banners with applicable DoD CUI rules will be displayed during logon to any ARIA Group asset, or when you authenticate into an ARIA Group system from an alternate working location. Privacy and Security notices will undergo a legal review. The ARIA Group Privacy and Security Banner will state: UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This computer system is the property of the ARIA Group Corporation. By using this system, users acknowledge notice of, and agree to comply with the ARIA Group Corporation Acceptable Use of Assets Policy and Information Security Policy. Use of this system which may include access to Controlled Unclassified Information (CUI) or Covered Defense Information (CDI), constitutes consent to monitoring which may be conducted for the protection against improper or unauthorized use or access. Disclosure, copying, dissemination, or distribution of CUI/CDI to unauthorized users is prohibited under CFR 32 Part 2002, and you agree not to disclose, copy, disseminate or distribute CUI/CDI to any unauthorized personal. Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated.

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

ARIA Group assets are manually configured to initiate a session lock with a pattern hiding display after 10 minutes of inactivity. The configuration is not in compliance with the STIG, which are security

guidelines provided by Defense Information Systems Agency (DISA). To comply with the STIG, ARIA Group assets will be controlled by EntraID and Intune Policies that enforce this control.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Sessions on ARIA Group end user computing devices will automatically log off at 2300 Pacific Time (PT). Network sessions including remote access sessions will be terminated at 2330 PT.

3.1.12 *Monitor and control remote access sessions.*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All remote sessions to the ARIA Group Enterprise Network for users, both standard and privileged, will be logged by an ARIA Group Security Information and Event Management (SIEM) system, and controlled via automated protocols. Suspicious activity (i.e., unknown asset attempting to authenticate to ARIA Group Enterprise Network, Foreign IP attempt to authenticate/scan or probe remote access sessions) will be immediately reported to an ARIA Security Incident Response Team (SIRT) to investigate, and an accompanying investigation or incident report will be delivered to the ARIA Group Information Security Committee. Indicators of compromise will be reported and escalated to the SIRT team. Upon confirmation of a compromise, the ARIA Group Security Incident Response Plan will be set in motion and followed.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ARIA Group will utilize an approved Advance Encryption Standard (AES) with a key length of 256 bits (AES-256)/FIPS 140-2 compliant algorithms for all encryption storage and communication requirements. Remote access sessions will utilize FIPS compliant certificates. All network assets are FIPS compliant and operate in a “FIPS MODE” which meets the medium assurance requirements for

FIPS 140-2. Prior to the deployment of new hardware, IT will harden assets and applications by applying the appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) using Intune policies. The ARIA Group Information Security Committee will conduct a monthly validation to ensure FIPS compliance. AES-256 supports the largest bit size and is practically unbreakable by current super computing power, making it the strongest encryption standard. AES-256 encryption methods are employed for transmission and storage of data containing CUI.

3.1.14 *Route remote access via managed access control points*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Some remote access (i.e., remote session connected with an ARIA Group Corporate owned device) is routed via secure managed access control points and authenticated by EntraID. In the future, all remote access will be authenticated by EntraID. Only authorized users can remote access the ARIA Group Enterprise Network. A username, password, and Multi-Factor Authentication (MFA) authenticator are used to authenticate the user prior to granting remote access to the Microsoft 365 environment, and all ARIA system will authenticate using this policy in the future. All remote access sessions will be logged and reviewed monthly by the ARIA Group Information Security Committee.

3.1.15 *Authorize Remote Execution of Privileged Commands*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The remote execution of privileged commands is not possible at ARIA Group today. In the future, remote execution of privileged commands will only execute with an authorized privileged account though Microsoft Intune, or an account assigned to a System Administrator for support of maintenance purposes, customer service, or deployment and integration activities. All remote activities for users and administrators will be logged by the ARIA Group SIEM and reviewed at least monthly by the ARIA Group Information Security Committee in the ARIA Group MRMM. All security-relevant information will be stored in a user access-controlled environment and granted on a least-privileged access basis to reduce the attack surface.

3.1.16 *Authorize Wireless Access Prior to Allowing Such Connections*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All wireless access at ARIA Group requires a password and Service Set Identifier (SSID). Wireless networks employ WPA2 and a non-vulnerable AES encryption protocol. No unauthorized or anonymous accounts are granted wireless access to the ARIA Group Enterprise Network. Guest Access is provided outside the ARIA Group Enterprise Network on a segregated wireless network and only granted for visitors to ARIA Group Facilities upon their request. In the future, wireless networks will employ WPA2 Enterprise, and access will authenticate using approved EntraID User IDs, passwords, and will require MFA using Microsoft Authenticator.

3.1.17 *Protect wireless access using authentication and encryption.*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All wireless access is protected utilizing authentication and encryption protocols (WPA2) and requires a pre-shared-key (PSK). Each ARIA Group facility has its own, dedicated wireless networks with separate Corporate and Guest networks. In the future, access to the ARIA Group Enterprise wireless network will require an active ARIA Group EntraID User ID, password, and MFA authenticator. Access to the Guest network requires a PSK. All wireless traffic is encrypted.

3.1.18 *Control connection of mobile devices*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Access to the ARIA Group Enterprise Network via authorized mobile devices will be controlled and monitored through the use of Intune, a Mobile Device Management (MDM) tool that will be installed on each authorized device. Mobile device users will have limited access to the ARIA Group Enterprise Network and are governed by internal corporate policy and User Agreements. The list of authorized

mobile devices will be reviewed and approved monthly by the ARIA Group Information Security Committee.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Only corporate issued laptops which utilize AES-256 encryption and are enabled with BitLocker for mobile computing platforms will be authorized to handle CUI. The Key Management will be centralized in EntraID. ARIA Group will utilize Intune for MDM to encrypt CUI on mobile devices.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All connectivity to any external systems or networks will be logged, documented, and approved prior to establishing connectivity. All connectivity to any external system or network will be logged and reviewed monthly by the ARIA Group Information Security Committee.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The use of personal or non-ARIA Group purchased USB portable storage devices at ARIA Group will be prohibited. Exceptions will be granted only if the Information Security Committee has identified an approved business need for the use of a portable storage device. Any portable storage device approved for use must be procured by ARIA Group from an approved vendor, inventoried by ARIA Group and digitally encrypted and tracked by EntraID.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Presenting or displaying CUI on publicly accessible systems will be prohibited by the AIRA Group Information Security Policy. The ARIA Group policy regarding social media and web management will require all public Internet postings to be reviewed and approved by the ARIA Group Executive Leadership to verify that the content does not contain CUI.

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

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Insider Threat training is provided to all new employees during onboarding and all employees on an annual basis. Administrators and stakeholders in the Insider Threat Program receive annual specialized training which addresses the administrative and technical aspects of the program as well as their reporting responsibilities. The Insider Threat Program undergoes an annual self-inspection by the ITPSO which is annotated in the Insider Threat Plan.

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

Audit logging is currently utilizing default settings in every system at ARIA Group. In the future, multiple sources will be used to audit and monitor the ARIA Group Enterprise Network which will allow for a complete monitoring snapshot. Audit log copies from network devices (syslogs), network packet inspections, Microsoft 365, and internal assets will be centralized and processed by a SIEM Data Processor. Logs will be retained for at least 90 days. The results will be presented at each Monthly Risk Management Meeting (MRMM) as part of the standing Agenda under the topics of Vulnerability and Threat Review.

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

Shared accounts are used on ARIA Group end user computing devices today. In the future, all system user and administrator activities will be traced and audited utilizing several toolsets to monitor activities while operating within the ARIA Group Enterprise Network. Logging at the system level will be accomplished via a special auditing policy controlled by Intune which retains security, application, and system level data for 90 days. Users and Administrators will be advised that all activities are logged, monitored and reviewed via company policy. All logging will be access-controlled to ensure no modifications or deletions of system logs occur.

3.3.3 *Review and Update Logged Events*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All security logs will be reviewed on a monthly basis with security events being identified for review during the course of the month. Anomalies are identified and immediately investigated by the SIRT team. The monthly review is a culmination of smaller reviews within the ARIA Group SIEM and endpoint detection and response (EDR) throughout the month which identify vulnerabilities and exploits as well as unauthorized user behaviors.

3.3.4 *Alert in The Event of An Audit Logging Process Failure*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The ARIA Group SIEM will identify and report logging failures to both IT System Administrators and SIRT team. The ARIA Group Information Security Committee will review a report showing audit log health including logging failures or success during the ARIA Group MRMM.

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

The future audit record review will contain adequate information which supports investigations, cyber forensic analysis, and calibration of misconfigured equipment. Audits will be completed at least monthly by the ARIA Group Information Security Committee during the ARIA Group MRMM.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The ARIA Group SIEM will allow for the reduction of a compiled security report for review for on-demand analysis and investigations by the SIRT team. The reports will be reviewed at least monthly by the ARIA Group Information Security Committee during the ARIA Group MRMM. Logs will be retained for at least 90 days.

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

All internal system clocks will be synchronized to approved ARIA Group Servers which receive system time from the following authoritative sources, NIST Nuclear Server and the GPS Time Server from the United States Air Force. These times are considered official, and the only deviation authorized is no greater than 5 mins lag in system time.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Only System Administrators will have access to the audit logs and audit logging tools. Audit logs will only be viewed by authorized System Administrators, members of the SIRT team, and the ARIA Group Information Security Committee. Logs will be read-only, and deletions are not authorized. Access controls for the audit records will be routinely reviewed.

3.3.9 *Limit Management of Audit Logging Functionality to A Subset of Privileged Users*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Only specific IT System Administrators, members of the SIRT team, and ARIA Group Information Security Committee members have access to view audit logs. Only the ARIA Group Information Security Committee and SIRT team can perform the audits and investigations. All investigations will have a corresponding report which is delivered to ARIA Group leadership and IT management.

3.4 Configuration Management

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

ARIA will maintain a secure baseline configuration for all assets within the ARIA Group Enterprise Network. These baselines will be hardened in accordance with the STIGs and Center for Internet Security (CIS) Benchmarks. Any deviations to these frameworks require approval from the Security

Officer. All deviations will be documented and carefully evaluated to identify potential risk within the ARIA Group Enterprise Network.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ARIA Group assets are hardened to applicable STIGs using a combination of Intune policies and manual one-time administrative configurations. All ARIA Group assets are scanned at least once a week by the Security Conformance Automation Protocol (SCAP)-compliant vulnerability management system.

3.4.3 *Track, Review, Approve or Disapprove, and Log Changes to Organizational Systems*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

The AIRA Group IT department will maintain configuration management standards for ARIA Group's IT organizational systems and ensures all changes are carefully evaluated and approved prior to deployment to the operational environment. IT changes control records, including ARIA Group change logs, will be audited on an annual basis by an independent third-party audit. All system changes will be documented and deviation requests for systems or assets not meeting system requirements will be submitted to the Information Security Committee for review and approval.

3.4.4 *Analyze the Security Impact of Changes Prior To Implementation*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Future changes will go through a Risk Assessment prior to approval and execution. The Risk Assessment results will be documented in the IT change control log. Change controls will be reviewed by IT management at least monthly, and the change log is reviewed by the ARIA Group Information Security Committee at least quarterly.

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

All proposed changes to ARIA Group's IT organizational systems will be carefully evaluated to ensure the changes do not negatively impact the company's user community and operations and follow the change management standards documented in controls 3.4.3 and 3.4.4.

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

All IT organizational systems will be configured to employ the least privilege principle and only essential capabilities are provided to both users and administrators. All Operating System will be hardened to applicable STIGs prior to use by an end user.

3.4.7 *Restrict, Disable, Or Prevent the Use of Nonessential Programs, Functions, Ports, Protocols, and Services.*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Nonessential programs, ports, functions, and services will be disabled as part of the STIG hardening security baseline. Restrictions will apply to both users and administrators. This information will be validated with at least weekly SCAP-compliant vulnerability scans, which are reviewed at least monthly by the ARIA Group Information Security Committee in the ARIA Group MRMM. Vulnerability reports will be reviewed at least monthly by the ARIA Group Information Security Committee to ensure disabled services and capabilities are not reintroduced and re-enabled.

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

Whitelisting and Blacklisting of Software will be implemented utilizing Intune. Blacklisted software shall not be allowed to reside or be used (executable function) within the ARIA Group Enterprise.

3.4.9 *Control and Monitor User-Installed Software*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Only authorized IT System Administrators will be permitted to install software on user assets. The inventory of installed software applications shall be reviewed at least annually by the ARIA Group Information Security Committee. When software is no longer required, the end-user must notify IT and the software will be removed remotely.

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

All Users and associated processes will be identified along with any devices which require elevated privileges in order to execute properly and documented in the ARIA Operating System (AOS). ARIA Group management has access to AOS and ARIA Group tickets are reviewed by both IT and ARIA Group management at least weekly. New applications or hardware related services are added the documentation is updated. The Business Information Systems Map (BISM) is maintained by the Chief Technology Officer (CTO) and Security Officer.

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

All users and processes will be authenticated by the ARIA Group Endra ID tenant prior to allowing access to the ARIA Group Enterprise Network.

3.5.3 *Use multifactor authentication for local and network access20Fto privileged accounts and for network access to non-privileged accounts.*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Multi-Factor Authentication (MFA) for local and network access will be accomplished through the use of EntraID and the Microsoft Authenticator. Users and Administrators will be required to utilize MFA for access to the ARIA Group Enterprise Network. There may be instances where a user has forgotten their Microsoft Authenticator device, in which case they contact IT and after ARIA Group Executive Leadership approval, the account is set to "by-pass" which will allow the user to authenticate without using Microsoft Authenticator.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Technical mechanisms shall be put in place to prevent "copy and paste" of credentials and passwords across privileged and non-privileged accounts. A user or administrator must enter the logon credentials for each account being accessed.

3.5.5 *Prevent Reuse of Identifiers for a Defined Period*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Disabled ARIA Group user accounts are left disabled in EntraID for a period of at least one year to prevent reuse. ARIA Group Human Resources (HR) maintains a list of employee employment dates and is referenced for any re-hire actions as part of the approval process.

3.5.6 *Disable Identifiers After a Defined Period of Inactivity*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Accounts are will be disabled after 45 days of inactivity. For users on short or long-term disability for FMLA, a comment may be placed in EntraID with the authorized return date and the account will only be re-enabled after HR approval. For all other accounts, approval from ARIA Group Executive Leadership will be required for reactivations.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Passwords are required to meet complexity requirements as defined by Microsoft, but not as defined in the DISA STIG/SRG. This policy is enforced via EntraID on some systems when new passwords are created and when updates are executed. Passwords must be at least 8 characters long, and contain at least 2 complexities (i.e., capital letter, number, and authorized symbol). One-time passwords will be used on an initial authentication only so Users must change their password after the first authentication.

3.5.8 *Prohibit Password Reuse for A Specified Number of Generations*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Passwords will be prohibited from reuse for 24 generations, which is enforced via a EntraID CAP.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Temporary passwords shall be generated for new users and after logging in for the first time, users are prompted to change their temporary password. The user's password must meet the organizational password complexity requirements.

3.5.10 *Store and transmit only cryptographically-protected passwords.*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Passwords are cryptographically protected when stored or transmitted within the ARIA Group Enterprise Network. This is enforced via EntraID.

3.5.11 *Obscure Feedback of Authentication Information*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Authentication information is obscured from visibility during logon actions to web, system, and network assets. This action will be enforced via Intune and EntraID policies.

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

ARIA Group will write a detailed Incident Response Plan which will include Defense Industrial Base (DIB) registration and validation, and annual exercise activities. The preparation, detection, analysis, containment, recovery, and user response activities will be documented specifically in the Incident Response Plan. The Security Officer and Contract Administrator will submit incident reports to the Defense Industrial Base Network (DIBNER) and the Defense Counterintelligence Security Agency (DCSA). Some incident reports will be shared with customers or law enforcement agencies such as the Naval Criminal Investigative Service (NCIS) or FBI.

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

In accordance with ARIA Group's future Incident Response Plan, all incidents will be documented and tracked internally, and all information and/or hardware is accounted for in a Chain of Custody Form which identifies the designated officials at the gaining organization for the positive control of the information/hardware.

3.6.3 *Test the Organizational Incident Response Capability*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ARIA Group's incident response capability will be tested at least annually. Individual restoration activities, such as recovery from backups, will be documented to demonstrate successful restoration from backup is possible..

3.7 Maintenance

3.7.1 *Perform Maintenance on Organizational Systems*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Maintenance is conducted on all organizational systems including databases and Cloud instantiations. ARIA Group does not have a Vulnerability Management policy that addresses the specific frequency in which maintenance is performed on the organizational systems and cloud instantiations. Most maintenance is performed by background-checked System Administrators. All System Administrators are U.S. citizens.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Only System Administrators are permitted to perform system maintenance. All system maintenance is performed manually or using built-in Operating System tools such as Windows Update. Administrative rights are provided to all users but will be limited to System Administrators to access this level of information.

3.7.3 *Ensure Equipment Removed for Off-Site Maintenance Is Sanitized of Any CUI*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All memory and system storage devices shall be sanitized (via an NSA approved procedure) from the hardware prior to shipment back to the manufacturer. There is no exception to this process. Memory and hard drives which are no longer required are destroyed via a certified destruction process.

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

All media will undergo a malware scan prior to introduction to the ARIA Group Enterprise Network. Media flagged with vulnerabilities will not be allowed to be introduced into the ARIA Group Enterprise Network. All findings are documented.

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

Multi-Factor Authentication (MFA) will be deployed across the ARIA Group Enterprise Network to include Administrator and User level accounts utilizing FIPS 140-2 compliant encryption. When

nonlocal maintenance is accomplished, external network connections will be terminated by administrators.

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All maintenance activities performed by personnel that do not have the required access authorization are closely supervised by authorized personnel. Technicians performing such activities are logged as visitors. All non-employee maintenance technicians (vendors) are closely supervised and escorted. Vendors must leave any camera devices including Smartphones at reception while onsite.

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

All CUI products, both digital and paper based will be physically controlled and stored when not in use. Once the CUI is no longer needed, it will be destroyed utilizing an approved destruction device or service. Hard drives and system media slated for destruction will be secured and in coordination with IT for sanitization and destruction will be logged.

3.8.2 *Limit Access to CUI on System Media to Authorized Users*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Access to CUI on system media is restricted to authorized users per organizational policy. In the future, access to CUI will be restricted inside of ARIA Group based on the need to know.

3.8.3 *Sanitize or Destroy System Media Containing CUI Before Disposal or Release for Reuse*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

System media containing CUI will be sanitized prior to reuse or destroyed when taken out of service. The asset will be documented and authorized for release and reuse by the CTO using a NIST 800-88-compliant Certificate of Sanitization (CoS). System media which cannot be sanitized due to hardware failure or media taken out of service is documented and destroyed.

3.8.4 *Mark Media with Necessary CUI Markings and Distribution Limitations*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All system media to include paper products will contain the appropriate CUI markings and distribution statements.

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

Positive accountability for all CUI materials will be enforced outside of controlled areas. Access will be restricted based on the "need-to-know" for all CUI/CDI data. All employees will receive CUI Handling Training via the Annual Security Refresher Training and job aides are provided to users and administrators via the ARIA Group Portal.

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

Cryptographic mechanisms will be implemented within the ARIA Group Enterprise Network to include applications which are FIPS 140-2 compliant. Network assets operate in FIPS Mode and AES-256 encryption methods are employed for transmission and storage of data containing CUI.

3.8.7 *Control the Use of Removable Media on System Components*

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All removable media on system components shall be disabled. ARIA Group users are not authorized to use unencrypted removable hard drives, thumb drives or other personally procured data storage devices. All requests for encrypted drives are submitted via ticket request and procured by IT after ARIA Group approval.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

Portable storage devices which are not approved encrypted ARIA Group or IT assets are not authorized for use within the ARIA Group Enterprise Network will be prohibited via both company policies and Intune policies. The policy shall be promogulated to users via the Annual Security Refresher Training.

3.8.9 *Protect the Confidentiality of Backup CUI at Storage Locations*

☒ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All backups are encrypted and secured digitally in ARIA Group's Irvine data center with very restrictive physical and logical access controls in place to ensure access to ARIA Group data is limited to required personnel. ARIA Group backups are encrypted in transit and at rest, and access controlled.

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

ARIA Group employees undergo pre-employment background investigations. ARIA Group background screening reports are stored by Human Resources.

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

All employee actions will be tracked by AOS, and access is immediately revoked by IT System Administrators for users who depart the organization upon formal notification. For users who transfer to another group/project, an IT ticket shall be submitted by their manager, a review of the user's access is conducted, and any unneeded access is removed prior to their new assignment. Personnel shall be required to sign ARIA Group forms attesting to no longer having Information Assets such as CUI or storage devices in their possession or custody when leaving ARIA Group.

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

Physical access to ARIA Group's servers and communications equipment is limited to authorized individuals employed by ARIA Group. Any unauthorized personnel must be logged at reception and be supervised by an authorized ARIA escort.

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ARIA Group has various physical security and access control measures in place in all facilities (e.g., alarms, cameras, cypher locks, and digital access control systems) which provide a layered approach to facility security. Alarm codes are issued to select personnel who are entrusted with after-hours/non-standard access.

3.10.3 *Escort Visitors and Monitor Visitor Activity*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All visitors must sign into a visitor logbook and are escorted by permanently assigned staff and appropriately badged prior to gaining access to a facility. Any maintenance from vendors is observed by permanently assigned staff and suspicious activities are reported immediately to facilities.

3.10.4 *Maintain Audit Logs of Physical Access*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All physical access logs are maintained digitally for at least <> days.

3.10.5 *Control and Manage Physical Access Devices*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All physical access controls for devices are limited to ARIA Group personnel. Only authorized ARIA Group have physical access devices allowing access to ARIA Group facilities. The production manager maintains an inventory of personnel who have a physical access device, such as a digital keycard or brass key.

3.10.6 *Enforce Safeguarding Measures for CUI at Alternate Work Sites*

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All work accomplished at alternate sites such as authorized home working locations requires approval. On an annual basis, all ARIA Group employees who have alternate working access will be trained on secure remote teleworking. All ARIA Group and IT assets will be encrypted at rest using AES 256-bit or higher encryption.

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

ARIA Group's Cybersecurity Risk Assessment procedure identifies how risk is accepted for hardware and software procurements and network configurations as well as identification of approved deviations. Data Handling controls which require government approval are formally submitted and documented under the Configuration Management policy and risk is re-evaluated no less than monthly to ensure requirements exist to support the deviation or approval in place. Formal organization-wide security risk assessments are conducted at least quarterly by the ARIA Group Information Security Committee.

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

The ARIA Group Enterprise Network is scanned for vulnerabilities and exploits at least weekly. Per ARIA Group's Vulnerability Management policy, all critical and high-risk exploits are immediately addressed and documented. ARIA Group, IT and Inovo participate in the NSA, DISA and CISA-DHS

alerts and notifications are acknowledged by the ARIA Group Information Security Committee at least monthly.

3.11.3 *Remediate Vulnerabilities in Accordance with Risk Assessments.*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ARIA Group's Vulnerability Management Policy requires that all vulnerabilities be addressed by IT System Administrators and Inovo security professionals after careful evaluation of the vulnerability and a Risk Determination made to the ARIA Group Information Security Committee to address how the vulnerability will be mitigated or accepted. The operational impact to internal users and clients is closely evaluated against the identified risks prior to implementation of mitigations.

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

ARIA Group's Risk Management Policy requires security controls to be continuously monitored and evaluated for compliance utilizing manual and automated methods. Control assessments are reviewed and discussed by the ARIA Group Information Security Committee at least quarterly.

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

ARIA Group's IT Vulnerability POA&M is maintained and regularly reviewed to ensure items are tracked, mitigated, and remediated in a timely fashion. The POA&M is utilized to track all Information Technology and cyber weaknesses identified through Security and Risk Assessments in addition to compliance-based actions such as NIST SP800-171 controls.

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

All security control requirements are actively monitored both manually and via automated methods to ensure compliance is maintained within the ARIA Group Enterprise Network. The ARIA Group Information Security Committee meets at least monthly to review reports on the monitoring of control activities. As ARIA Group approved changes are made within the ARIA Group Enterprise Network, a Risk Assessment is performed by the ARIA Group Information Security Committee to ensure other security controls are not impacted by the changes.

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

ARIA Group's System Security Plan (SSP) is updated and reviewed frequently as part of our Configuration Management and Risk Assessment processes to ensure system requirements and security plans are accurately documented.

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

All communications are monitored and controlled at the external key internal boundaries by the SIEM and ARIA Group Information Security Committee. The Network Diagram depicts flow control of data and identifies the network assets by make and model as well as a redacted IP address.

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

ARIA Group employs effective information security for all systems within the ARIA Group Enterprise Network, all architecture designs are reviewed to ensure system security engineering principles are adhered to. All ARIA Group network infrastructure including Firewalls, Servers, Software as a Service, and Switches are to be hardened to current DoD STIGs. ARIA Group currently does not develop software. If ARIA Group were to develop software, the software development would comply with the Company Software Development Plan, Procedure, and Secure Coding Standards.

3.13.3 *Separate User Functionality from System Management Functionality*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All ARIA Group User permissions are restricted to ensure least privilege is adhered to and users do not have administrative privileges. Authorized IT System Administrators use privileged accounts for conducting administrator level functions within the ARIA Group Enterprise Network. Privileged accounts are audited and reviewed at least monthly by the ARIA Group Information Security Committee.

3.13.4 *Prevent Unauthorized and Unintended Information Transfer Via Shared System Resources*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Unauthorized and unintended information transfer is prohibited by the ARIA Group Information Security Policy. All computer assets are assigned to an ARIA Group user who is accountable for ensuring other ARIA Group personnel do not log into their asset without their supervision. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

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

Subnetworks for publicly accessible system components are logically separated from the network. Access to the subnetworks is limited to select individuals supporting web hosting and development activities.

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

All network communications traffic from ARIA Group facility networks are configured to allow traffic by exception. Remote assets must use Operating System firewalls to deny network communications traffic by default.

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

All remote sessions are configured to only allow one session per user at a time. Split tunneling is disabled on all ARIA Group Enterprise Network Virtual Private Network (VPN) servers.

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

Cryptographic mechanisms have been implemented to prevent the unauthorized disclosure of CUI during transmission, all emails are encrypted utilizing AES-256 compliant algorithms and FIPS 140-2 compliant hardware which operate in FIPS mode.

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

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

All network connections associated with communications sessions must terminate after an agreed-upon defined condition, such as a period of inactivity or time of the day.

3.13.10 *Establish and manage cryptographic keys.*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All keys which are employed within the ARIA Group Enterprise Network are managed, protected, and centrally stored to ensure a compromise does not occur. IT has established and manages the ARIA Group Enterprise Network cryptographic keys for cryptography employed in ARIA Group systems.

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

FIPS validated cryptography is utilized to protect the confidentiality of CUI within the ARIA Group Enterprise and only approved encryption algorithms are in place.

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

Collaborative computing devices are prohibited from use on ARIA Group Enterprise Networks.

3.13.13 *Control and Monitor the Use of Mobile Code*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ARIA Group monitors for the use of vulnerable mobile code utilizing SCAP-compliant vulnerability scans. This activity is monitored by the ARIA Group Information Security Committee, and any exploits relating to mobile code within the ARIA Group Enterprise Network are reviewed at least monthly. A risk assessment is performed by the committee if mobile code is in use, and vulnerabilities including exploits are remediated by IT unless the risk is accepted.

3.13.14 *Control and Monitor the Use of Voice Over Internet Protocol (VoIP) Technologies.*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All VoIP is controlled and monitored at ARIA Group. The organization utilizes VoIP for voice communications which is provided by 8x8 communications VoIP devices and traffic are segregated on a subnetwork that does not have access to the ARIA Group Enterprise Network.

3.13.15 *Protect the Authenticity of Communications Sessions*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All electronic communications sessions are encrypted, and electronic authentications are verified by Multi-Factor Authentication and USERID and password. Accounts are monitored by the SOC for spoofing based off the application of artificial intelligence and cyber threat analysis capabilities. Communication sessions are categorized based on the MITRE ATTAK Framework and reviewed at least monthly during the ARIA Group MRMM by the ARIA Group Information Security Committee. For electronic mail addresses which may be compromised or impersonated by an external party, the user will notify the FSO and IT. The FSO will notify the SIRT Team to investigate the addresses or indicators of compromise. The FSO will coordinate with Communications Carriers, ISPs, Federal Resources and Email Hosts if an account is believed to be compromised. If an ARIA Group account is believed to be compromised, IT will revoke active session keys, rotate the password, and the SIRT team will perform a forensic investigation proving what the intruder did during the breach, or proving that the account was not compromised.

3.13.16 *Protect the Confidentiality of CUI at Rest*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

To protect CUI at rest, all computers and servers are BITLOCKER enabled with the key management being encrypted and access controlled.

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

All system vulnerabilities and exploits are identified and remediated in accordance with the ARIA Group Cybersecurity Risk Management procedure. Vulnerability reports are generated weekly and reviewed at least monthly by the ARIA Group Information Security Committee. All Critical and High Vulnerability exploits are to be addressed immediately but no later than 14 days from notification from the DHS CIRT, which has the cognizant authority for the US Government for Cyber Alerts and the mitigations documented. Moderate Vulnerability exploits are addressed within 30 days.

3.14.2 *Provide Protection from Malicious Code*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The ARIA Group Enterprise Network provides protection from malicious code at designated locations within organizational systems using CrowdStrike malware protection enabled on all servers and computers. Spam Titan monitors for and removes email attachments that contain malicious code. The

malware scans occur on a constant basis and the software configuration is optimized and validated annually. Malware reports are reviewed at least monthly by the ARIA Group Information Security Committee.

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

The organization is subscribed to CISA-DHS, CERT, DISA, FBI and NSA advisories and acknowledges CYBERCOM advisories and warnings as they are released. The company policy also prescribes that all DIB notifications and INFRAGARD advisories be acknowledged as well.

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

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Malware code protection from Crowdstrike is automatically updated and those updates are forced out to the agents in real time to ensure protection of assets is accomplished without user notification or acknowledgement. Notifications have been enabled to IT to advise when the malware protection settings are changed, or an agent is failing to operate properly. Reports on malware status are reviewed at least monthly by the ARIA Group Information Security Committee.

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

Scans of all ARIA Group Enterprise Network systems for download of all files or folders are accomplished via Crowdstrike, no outside files can be introduced either from the web or removable

media without first undergoing a scan prior to accessing the information. Electronic mail is screened for malware by SpamTitan prior to delivering the electronic mail to the user's mailbox.

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

All systems are protected at internal and external firewall points and monitored by the SIEM and SOC for inbound and outbound traffic. GEO FENCE rulesets are applied to all nation state countries and IPs which have been identified as threats from validated law enforcement and intelligence communities.

3.14.7 *Identify Unauthorized Use of Organizational Systems*

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

All system use is monitored to include web browsing and movement of large data sets across the ARIA Group Enterprise Network to either removable media or attempts to send the information externally to personal email addresses. The technical controls implemented are part of the Insider Threat Monitoring and the Insider Threat Policy, monitored by the SIEM and SOC, and reviewed at least monthly by the ARIA Group Information Security Committee.

APPENDIX A – NETWORK DIAGRAMS