DEPARTMENT OF MILITARY AFFAIRS
Office of Inspector General

St. Francis Barracks
P.O. Box 1008
St. Augustine, Florida 32085-1008

JLAC received 9.28.2024

August 28, 2024

Ms. Melinda Miguel
Chief Inspector General
Office of the Chief Inspector General
Room 1902 – The Capitol
Tallahassee, Florida 32399-0001

Dear Ms. Miguel:

Pursuant to Section 20.055(6)(h), Florida Statutes, enclosed is the Department of Military Affairs' response on the corrective actions taken in connection with the Auditor General's Report No. 2024-134, dated February 20, 2024.

If you have any questions, or require additional information, please contact me at (904) 823-0126.

Sincerely,

Jennifer L. Ranick
Inspector General
Department of Military Affairs

Distribution:
Kathy DuBose
Joint Legislative Auditing Committee Coordinator
Sherrill Norman
Auditor General of Florida
MG John D. Haas
The Adjutant General
COL Adam Curry
State Quartermaster

DEPARTMENT OF MILITARY AFFAIRS

Office of Inspector General

August 28, 2024

The following represents the status of those recommendations included in the Auditor General Report, dated February 20, 2024, entitled "Department of Military Affairs Selected Administrative Activities".

Recommendation No. 1: To promote the independent assessment and oversight of cybersecurity program controls, we recommend that Department management ensure that the Department's designated ISM is organizationally separated from the Department's daily IT operations.

Actual or Proposed Corrective Action: The agency head for the Florida National Guard/DMA (The Adjutant General) will appoint the G6/Information Systems Security Manager (ISSM) as the agency ISSM. The ISSM will serve as a direct report to the Florida National Guard G6/CIO for all issues, apart from non-compliance and incident response. The ISSM will report all issues of non-compliance or incident response directly to The Adjutant General and the G6/CIO.

6 Month Status: A memorandum of record was generated and signed by the current Adjutant General, Major General John D. Haas, on 29 February 2024. A separate individual has been designated as the Information System Manger for the DMA. In accordance with Florida statues, section 282.318(4)(a), the designated ISM will report noncompliance and cybersecurity threats and incident response efforts to the agency head in conjunction with the DMA G6/CIO.

Finding No. 1 has been fully corrected.

Recommendation No. 2: We recommend that Department management work with the United States Department of Defense to establish procedures for retaining all text messages sent or received by Department-owned mobile devices in accordance with State law.

Actual or Proposed Corrective Action: The Florida National Guard G6/CIO issued a policy on 19 August 2022, forbidding the sanitization of Department of Defense and Department of Military Affairs (DMA) mobile devices, until such time the Department could identify and procure an approved data retention solution. The published memo was meant to serve as a stop gap to the existing problem. The Florida National Guard, DMA G6/CIO continues to search for an approved enterprise solution that meets the state and federal regulatory retention requirements.

6 Month Status: The Florida National Guard currently utilizes MobileIron to provide unified endpoint and enterprise mobility management for mobile devices issued by the G6 to Federal and

State representatives for Department of Military Affairs. MobileIron does not have the ability to meet the current state regulatory retention requirements for digital text messages. The server and services are hosted and managed on premise at the Army Reserve National Guard (ARNG) Bureau in Virginia. ARNG contemplated the purchase of a supplemental enterprise solution called Cellebrite to enable the collection, review, and management of digital text messages. The solution did not receive final approval and was never implemented. Currently, a signed end-user license agreement (EULA) is collected for each phone issued by the G6. Signed EULA is acknowledgement by end user that all official business conducted on issued mobile devices are conducted on Microsoft TEAMs or Microsoft Outlook. The use of text messages is not an authorized form of correspondences for official business. Copy of all EULAs are on file with the G6 Mobility Manager.

Recommendation No. 3: We again recommend that Department management establish public deposit procedures to ensure that:

- Complete and accurate Forms are obtained for all public deposit accounts.
- QPD information is confirmed in accordance with State law.
- Annual reports are timely submitted to the CFO.

Actual or Proposed Corrective Action: The State Quartermaster (SQM) Resource and Accountability Management (RAM) office will update Florida National Guard (FNG) Pamphlet 210-4, which provides policy guidance for all Armory Operational Account (AOA) bank accounts and annual reviews. The FNG 210-4 will require all banking forms be reviewed annually for accuracy and completion during AOA Annual Reviews by the SQM RAM AOA audit reviewer. All discrepancies will be addressed and corrected by SQM personnel on site during the review. All new accounts will have the required QPD paperwork completed at the bank and reviewed by the SQM regional reviewer having oversight of the facility at the time of opening any new accounts to ensure compliance with state regulations.

6 Month Status: The State Quartermaster (SQM) Resource and Accountability Management (RAM) office is still in the process of updating the current Florida National Guard (FNG) Pamphlet 210-4, which provides policy guidance for all Armory Operational Account (AOA) bank accounts and annual reviews. As we now begin the 24-25 annual audit reviews, all discrepancies will be addressed and corrected by SQM personnel on site during the review. All new accounts will have the required QPD paperwork completed at the bank and reviewed by the SQM regional reviewer having oversight of the facility at the time of opening any new accounts to ensure compliance with state regulations.

Recommendation No 4.: We again recommend that Department management strengthen procedures to ensure that purchasing cards are promptly canceled upon a cardholder's separation from Department employment.

Actual or Proposed Corrective Action: Notification of out-processing requirements is currently being captured through DMA's Human Resource section and the employee exit interview and checklist upon departure. This check and balance will ensure purchasing cards are promptly canceled upon a cardholder's separation from DMA employment. This requirement will also be identified in the new HR Employee Handbook and is already identified in the supervisor training and HR desk reference for out-processing employees.

6 Month Status: Notification of out-processing requirements is currently being captured through DMA's Human Resource section and the employee exit interview and checklist upon departure. The new HR Employee Handbook is currently being drafted by State HR and is already identified in the supervisor training and HR desk reference for out-processing employees.

Recommendation No. 5: We recommend that Department management enhance policies and procedures to address processes for removing and sanitizing or physically destroying IT device hard drives prior to disposal, including requiring that Department records appropriately account for and evidence the sanitization or destruction of all surplus IT device hard drives.

Actual or Proposed Corrective Action: The Florida National Guard, DMA G6/CIO follows the appropriate state and federal guidelines for the sanitization and disposal of hard drives. However, we recognize that the lack of formal written policies outlining these procedures may result in risk. The Florida National Guard, DMA G6/CIO will codify all hard drive disposal processes in written policy, alleviating and associated risk of employees not knowing or understanding proper procedures and/or the unintentional loss or exposure of sensitive data.

6 Month Status: The Florida National Guard is drafting a policy that codifies the proper sanitization and disposal of hard drives to alleviate the risk of unintentional loss of sensitive data. In addition to policy, employee education and cyber awareness is key to alleviating risk on the network. DMA employees are required to complete annual cyber awareness training and sign an Acceptable Use Policy (AUP), which also addresses the need to protect sensitive data. Currently the DMA Network Manager, Information Security Analyst, and ISM meet bi-weekly to draft formal written polices for standard operating procedures on the DMA network.

Recommendation No 6.: We recommend that Department management establish policies and procedures requiring the completion of Checklists documenting the return of State-owned property by all employees separating from Department employment. In addition, Department management

should enhance employee training for and management oversight over the completion and retention of Checklists.

Actual or Proposed Corrective Action: Notification of out-processing requirements is currently being captured through DMA's Human Resource section and the employee exit interview and checklist upon departure. This will also be identified in the new HR Employee Handbook and is already identified in the supervisor training and HR desk reference for out-processing employees. Property Custodians will be assigned for each sub-department, as they verify the property through inventory as it is assigned to and from employees upon employment and separation.

6 Month Status: Notification of out-processing requirements are currently being captured through DMA's Human Resource section and the employee exit interview and checklist upon departure. The new HR Employee Handbook is currently being drafted by State HR and is already identified in the supervisor training and HR desk reference for out-processing employees. Property Custodians have been assigned for each sub-department.

Recommendation No. 7: We recommend that Department management enhance policies and procedures to require, in accordance with State law, the completion of conflict-of-interest attestations by all Department personnel taking part in the evaluation and selection process for noncompetitively procured contracts and purchase orders and that such attestations be maintained in Department records.

Actual or Proposed Corrective Action: DMA Contracting office will add an attestation form to the Contract Administrator's checklist. The Contract Administrator will ensure that any evaluator involved in the purchase over $35k will complete the attestation form. This signed form will become part of the documents in the file for that purchase and loaded into respective databases for record.

6 Month Status: DMA Contracting office has added an attestation form to the Contract Administrator's checklist. The Contract Administrator is ensuring that any evaluator involved in the purchase over $35k has completed the attestation form. Signed forms have become part of the documents in the file for that purchase and loaded in respective databases for record.

Finding No. 7 has been fully corrected.