TECHNOLOGY & INNOVATION
POLICE CAD (VERSATERM)
CONTROLS & APPLICATION REVIEW
AUDIT 18-11
October 5, 2018

CITY OF TAMPA

Bob Buckhorn, Mayor **Internal Audit Department**

Christine Glover, Internal Audit Director

October 5, 2018

Honorable Bob Buckhorn
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Police CAD (Versaterm) Controls & Application Review, Audit 18-11

Dear Mayor Buckhorn:

Attached is the Internal Audit Department's report on Technology & Innovation, Police CAD (Versaterm) Controls & Application Review.

We thank the aforementioned management and staff for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover
Internal Audit Director

cc: Dennis Rogero, Chief of Staff
Sonya Little, Chief Financial Officer
Ernest Mueller, Chief Assistant City Attorney
Russell Haupert, Chief Technology Officer
Martin Zinaich, Lead Systems Analyst
Johna Pleickhardt, MIS Project Leader
Brian Dugan, Chief of Police
Elias Vazquez, Assistant Chief of Police
Lee Bercaw, Deputy Chief of Police

TECHNOLOGY & INNOVATION
POLICE CAD (VERSATERM)
CONTROLS & APPLICATION REVIEW
AUDIT 18-11
October 5, 2018

/s/ Anthony D. Tiwari

Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION
POLICE CAD (VERSATERM)
CONTROLS & APPLICATION REVIEW
AUDIT 18-11

BACKGROUND

The Tampa Police Department (TPD) has been using an enterprise–level computer application since 2001, developed by a third party vendor Versaterm, to perform their daily operations. The vendor, a Canadian entity, provides the application as well as support to approximately 82 international law enforcement agencies including 31 here in the United States. TPD uses the operational functions of the application to communicate critical information to first responders. The technical aspects of the application are administered by a dedicated group within the Technology & Innovation Department (T&I). The application has four major components: Mobile Data Terminal (MDT), Mobile Report Entry (MRE) installed on police cars, Computer Aided Dispatch (CAD) used by the Communications Center and Records Management System (RMS) which allows TPD to access, capture, store and transmit Criminal Justice Information (CJI).

Data processed in Versaterm's MDT, MRE, and CAD is transmitted to RMS which is one of TPD's main records management systems. As the application contains critical CJI, it must be managed and protected according to the requirements set forth by the Federal Bureau of Investigation (FBI) through its Criminal Justice Information Services (CJIS) Security Policy. The policy provides a minimum set of security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI[1].

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY18 Audit Agenda. The objectives of the audit were to ensure:

1. The City of Tampa (COT)'s compliance with the FBI's triennial CJIS audit requirements.
2. Users with access to Versaterm's CAD and RMS applications are appropriate.
3. The adequacy of a current vendor risk management program for the application.
4. The change, issue management process, and user acceptance testing (UAT) guidelines are followed.
5. Physical access controls for Information Technology (IT) server equipment that contains CJI are adequate.

STATEMENT OF SCOPE

The audit period covered October 1, 2016, through May 31, 2018. Both qualitative and quantitative assessments were performed to determine whether the management and staff of T&I and TPD were fulfilling their stated duties and responsibilities in an effective and efficient manner. Original records as well as copies were used as evidence and verified through observation and physical examination.

1. CJIS Security Policy, Version 5.6. Approved by: CJIS Advisory Policy Board, 6/5/2017

STATEMENT OF METHODOLOGY

We achieved our audit objectives by utilizing the following methods:

1. Conducted interviews with the application administrators in both T&I and TPD to determine whether adequate controls over the internal processes have been established.
2. Reviewed the FBI's CJIS Policy to understand the minimum standards for protecting CJI.
3. Researched Control Objectives for Information and Related Technologies (COBIT 5) papers as a best practice framework for the governance and management of vendor supplied applications.
4. Reviewed T&I's internal policy and procedures manual to determine alignment to CJIS policy guidelines and best practices.
5. Performed a data reliability analysis to determine completeness and accuracy of system generated information.
6. Performed user access testing on all CAD and RMS users to determine the appropriate levels of access and segregation of duties.
7. Analyzed the contract and service level agreements between COT and Versaterm to determine the nature of contracted services.
8. Reviewed the applications change and issue management procedures to determine if internal processes were followed.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

AUDIT CONCLUSIONS

Based upon the audit work performed, our conclusions are as follows:

1. COT is in compliance with the FBI's triennial CJIS audit requirements; however, some areas can be improved.
2. The users with access to Versaterm's CAD and RMS applications are appropriate, but need to be reviewed periodically in accordance with CJIS policy requirements.
3. The current vendor risk management program for the application can be improved.
4. The change and issue management process are followed; however, UAT guidelines for documenting what is performed are not used.
5. The physical access controls for IT server equipment that contains CJI are acceptable.

COMPLIANCE WITH CJIS AUDIT

STATEMENT OF CONDITION: We reviewed the April 20, 2018, Florida Department of Law Enforcement (FDLE) CJIS technical audit, to verify COT's compliance to the polices and regulations of the Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC); adherence to the FDLE Criminal Justice User Agreement (CJUA) as well as the FBI's CJIS Security Policy (CSP); and to state and federal laws and administrative codes. We noted the audit contained four operating procedures that needed aligning to the CJUA and CSP.

CRITERIA: Per CJIS Policy, each CJIS System Agency shall, at a minimum, triennially audit all Criminal Justice Agencies which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies. Agencies that process and transmit CJI must meet the minimum compliance with the FBI's triennial CJIS audit requirements. Non-compliant area(s) must be responded to the FDLE CJIS Director in writing within 30 days.

CAUSE: TPD, in conjunction with T&I, has not aligned their internal controls to CJIS policy requirements, to safeguard, process and transmit CJI to the FDLE and various criminal databases through multiple devices and applications. The alignment of controls to CJIS policy is required, as TPD also accesses CJI via the FDLE's FCIC and the NCIC systems.

EFFECT OF CONDITION: Non-compliance or repeat findings with CJIS policy requirements, guidelines, and agreements for protecting the sources, transmission, storage, and generation of CJI results in sanctions imposed by the CJIS Advisory Policy Board. A lack of security over CJI could have a significant impact on the lives of citizens.

RECOMMENDATION 1: T&I and TPD should respond to the CJIS audit recommendations within the prescribed time frame; implementations in the response should be completed within the allotted timelines. T&I and TPD should consider conducting a periodic internal review of CJIS policy requirements to ensure compliance as the CJIS audit is performed, by the FDLE, every three years.

MANAGEMENT RESPONSE: Management concurs with the recommendations. T&I and TPD have and do respond to the CJIS recommendations within the prescribed period and complete implementations within the allotted timelines, except in rare cases where the cost or complexity of requirements necessitates a negotiated compliance timeframe. In these cases, we have fully communicated with and gotten approval of the regulating bodies.

It should be noted of the referenced CJIS Audit findings:

- Response 1B (remote vendor access outside the US) references a policy we cannot locate. FDLE was not able to produce the referenced policy. As such, we have asked for an extension and clarification. This is a finding where the material facts have not changed and this finding was not referenced in previous CJIS audits.

- Four other findings (disk encryption, multifactor, session lock and local firewall) are based on the fact that officers have a key to unlock the MDT from a physical car mount. Thus an inferred finding, during the audit, pushed the MDT into a different category of coverage from previous years. The below chart highlights their response dates and status of compliance.

TARGET IMPLEMENTATION DATE:

RESPONSE NUMBER & TITLE	BRIEF DESCRIPTION	STATUS & TARGET IMPLEMENTATION DATE
1A – Access Control	30 minute timeout to be applied on TPD officer MDT's.	Completed 8/30/2018
1B – CJI Accessible Data	Policy under review with FDLE leads. October 2018 Council meeting to determine response.	TBD
2 – Advanced Authentication	Multifactor Authentication Rollout.	6/30/2019
3 – Encryption for CJIS Data -	Adoption Plan to be created to support the effort of updating non encrypted hard drives. Expected implementation date is two years based on TPD sustainment plan rollout of 200 laptops per fiscal year.	1/30/2020
4 – Personal Firewall Protection	Update to be rolled out in parallel with 1A – Access Control.	Completed 8/30/2018

VERSATERM USERS ACCESS

STATEMENT OF CONDITION: Per analysis of the 522 active user's accounts with access to RMS, 128 accounts that have been disabled by Information Security in Oracle and Active Directory remained active in the RMS application. A user access review of the levels of application access has not been performed. Further noted, generic special privileged access rights accounts "Super User" and "Test Account" are configured in the application's production environment with an Active Directory profile and the highest level of privilege in both CAD and RMS applications.

CRITERIA: Per CJIS, 5.5.1 Account Management, the agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Per COBIT 5, DSS05.04 User Account Management, ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion, or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals. Ensure that all users (internal, external, and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable.

CAUSE: An access control list has not been generated from the application to conduct a periodic user access review for CAD and RMS user accounts. Inactive user accounts have not been disabled in the RMS application. The vendor's privileged access accounts have not been configured, to clearly define who the users are, in either CAD or RMS.

EFFECT OF CONDITION: Unauthorized individuals can gain access to active accounts and view/compromise sensitive CJI. Through a support agreement with the vendor and T&I, the vendor's development and maintenance team remotely accesses the applications to address issues and create updates. However, generic accounts are being used by the vendor and the individuals remotely logging into the application are not known.

RECOMMENDATION 2: T&I together with TPD should develop procedures for conducting a periodic user access review to evaluate the level of each user's access for both employees and contractors. Terminated employees or inactive user accounts held for historical purpose should immediately be disabled in the application. T&I should communicate with the vendor to update the title "Super User" and "Test Account" with the developer's names that have been CJIS certified.

MANAGEMENT RESPONSE: Management concurs with the observations and recommendations and is pleased with the recognition that general network, active directory and other contributing security procedures and policies are fully observed. We further understand that while up to this point application level security has been the responsibility of the application owner, T&I can play a role in ensuring the application owners meet these best practices.

The system as supplied has a facility to query and maintain internal application security and T&I/Oracle/HR currently supplies timely information on a weekly/monthly basis to address these needs.

To help the application owner ensure future compliance, T&I will meet with the application owners and our detailed step plan is recognized below.

TARGET IMPLEMENTATION DATES:

1) Activate User Validation in RMS and CAD –this will be an action item taken to secure that the inactive or disabled list from Security/Oracle matches the user count in the RMS application as a maintenance task. Based on the above, counts should be approximately 395 "active" users in the application user table. Process to create and build report, validate query data, terminate/expire active user accounts and produce report was completed on 8/1/2018.

2) Super User and Test Account transactions in CAD and RMS – COT will review the user role to role transactions as a second follow up based on completion of Task #1. Part of this solution will ensure that the VPN user's access remotely is attached also to one of these roles and can be identified by "individual name" on the role permission matrix. The assumption as named as well and confirmed against the CJIS audit is that all vendor accounts follow the security policy of the city and are required to have background and required checks as part of the CJIS certification. The role permission matrix for both CAD and RMS systems is scheduled to be completed on 3/30/2019.

3) Review period frequency and maintenance – current process from the T&I Security is to supply a facility to query and maintain internal application security, and the T&I Security Office supplies two different forms of notification to the application owner:

    1. Termination email notification – An email notification is sent to the application owner and designated backup whenever a TPD account is disabled.

    2. Weekly Change Reports emails – An email notification titled "Weekly Change Reports…" is sent to the application owner and designated backup. Each weekly notification contains 2 attached files:

        a. One file lists certain changes, including terminations, entered into Oracle by HR during the previous week.

        b. The second file lists all network accounts, including Police accounts, disabled by the Security Office during the previous week. This file also contains a 2nd worksheet listing any accounts which changed due to department transfer or network access being granted.

To help the application owner ensure future compliance, T&I will also build a report, review it quarterly and forward the details and recommendations to the application owner for action. These files will remain under the T&I shared folder (Audit accessible) and discussed with the application owner. Based on using the calendar year quarterly periods, the next documented review will be validated by T&I Security, approved and placed in the shared folder. This is scheduled to be completed on 4/30/2019.

INQUIRY ITEM	BRIEF DESCRIPTION	TARGET IMPLEMENTATION DATE
Active User Validation – Finding 1	Review CAD/RMS active user list against Security/Oracle inactive list. Validate user counts match in production.	Completed 8/1/2018
Super User and Test Account Training	Review user accounts under this role and validate account permissions against CJIS policy regulations.	3/30/2019
Long Term Maintenance or Process Review – Business and Customer Owned items.	Work with BA leads to create process and policy for long term maintenance of user accounts. Review and approved by T&I Security.	4/30/2019

VENDOR RISK MANAGEMENT

STATEMENT OF CONDITION: The contract executed in 1998 between the vendor, Versaterm and COT does not contain a "Right to Audit" clause, in order for the city to monitor the vendor's security and overarching compliance requirements. There has been no prior review of the vendor's internal controls or their financial health.

CRITERIA: Per COBIT 5, APO10.04 Manage supplier risk. Identify and manage risk relating to suppliers' ability to continually provide secure, efficient and effective service delivery. Per APO10.05, Monitor supplier performance and compliance. Periodically review the overall performance of suppliers, compliance to contract requirements, and value for money, and address identified issues; request independent reviews of supplier internal practices and controls.

CAUSE: The contract between the vendor, Versaterm, and COT does not contain an agreement for the city to examine the vendor's security and overarching compliance requirements. Per review of two other Versaterm clients' contracts, it was noted that the "Right to Audit" clause exists. T&I's administration has not adopted best practices to utilize a formal vendor/third-party risk management framework**.**

EFFECT OF CONDITION: The vendor may be exposed to data breaches, operational failure and bankruptcy. Inadequate controls on the vendor's network could allow security threats to COT as the vendor has authorization to access the applications production environment for maintenance and upgrades, which permits access to CJI.

RECOMMENDATION 3: T&I should communicate with the Legal and Purchasing Departments to amend the contract in order to allow greater transparency. T&I should select a vendor/third-party risk management framework to develop a program for monitoring third-party relationships, specifically those that involve critical activities with the potential to be exposed to significant risk. T&I should align the required policies, processes, and guidelines to the objectives of the program.

MANAGEMENT RESPONSE: Versaterm is a long-term vendor with a 20+ year history providing service to TPD/COT, with the contract last reviewed/renewed on 6/2004. While T&I does not specifically manage the Versaterm contract, we concur with the recommendation of adding a right to audit clause in subsequent renewals. It is our understanding that the audit rights suggested are typical for IT service providers delivering outsourced services with complex pricing arrangements, or hosted/SaaS arrangements – neither of which apply in this case for our on premises installation.

TARGET IMPLEMENTATION DATE: T&I will work together with TPD, Legal, Purchasing and the Vendor to propose a right to audit clause for future renewals. Based on the last addendum to the services contract being in June, we are requesting that 6/30/2019 be the targeted implementation date.

USER ACCEPTANCE TESTING

STATEMENT OF CONDITION: For FY17 changes and upgrades to the Versaterm suite of applications, T&I did not formally document UAT between the end user and T&I.

CRITERIA: For application changes and upgrades, the contract between the COT and Versaterm Systems details that the customer shall conduct the various acceptance tests. Per COBIT 5, Process Reference Guide BAI07, suggests to formally accept and make operational new solutions, including implementation planning, system and data conversion, and acceptance testing.

CAUSE: T&I and TPD have not adopted guidelines in the vendor's contract and industry best practices for documenting UAT and meeting end user expectations.

EFFECT OF CONDITION: There is no evidence that UAT has occurred and the software application may not behave as the end users anticipate. The vendor could be inundated by requests to resolve defects increasing the city's application support cost.

RECOMMENDATION 4: Create a test plan to perform and document assessments with the end user in order to determine that the application changes and upgrades perform in accordance with user requirements. Per COBIT 5, BAI07.03 Plan acceptance tests, establish a test plan based on enterprise wide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.

MANAGEMENT RESPONSE: Management concurs with the observations and recommendations and is pleased with the recognition regarding testing policies and procedures are further developed. We further understand that while up to this point application level testing practices have been the responsibility of the application owner, T&I can play a role in ensuring the application owners meet these best practices.

TARGET IMPLEMENTATION DATE:

1) Vendor contract validation of upgrade and UAT responsibility – action item generated was to review Versaterm maintenance contracts as is it applies to the vendor level of responsibility during upgrade projects. After review, specific questions around role and responsibility of upgrades and management of various acceptance tests were submitted to the vendor for response. Vendor confirmed their roles and responsibilities during a "vendor managed" upgrade and provided T&I with their supporting documentation. Completed 6/22/2018.

2) Implement the following inquiry items along with a brief description and target implementation date.

INQUIRY ITEM	BRIEF DESCRIPTION	TARGET IMPLEMENTATION DATE
Detailed test plan showing vendor application items that are city specific or required for implementation and testing (UAT based)	Create, deliver and maintain "Cobit" certified deliverables for test strategy, test cases, test planning & monitoring	3/30/2019
Acceptance Testing Progress and written Customer Admin POC/Signoff from Test to Production	Create, deliver and maintain user acceptance testing (UAT) documents that are "Cobit" certified.	3/30/2019
Post Upgrade/ Implementation Review of Production Issues	Create, deliver and maintain post implementation issues with detailed resolution paths.	3/30/2019