CJIS Incident Review
December 2015

Lori Brooks, City Auditor
Susan Edwards, Assistant City Auditor
Roshan Jayawardene, Internal Auditor

ARLINGTON
THE AMERICAN DREAM CITY
City Auditor's Office

December 21, 2015

Honorable Mayor and Members of the City Council:

At the request of the City Manager's Office, the City Auditor's Office has completed a review of a recent security issue related to Fire Department access to Criminal Justice Information Services (CJIS) data. The purpose of this review was to determine the extent and consequences of the security issue, as well as evaluate compliance issues related to the Computer Aided Dispatch System (CAD) Intergraph 9.3 software implementation.

We would like to thank the Arlington Fire Department, Dispatch Services, Arlington Police Department and Information Technology staff for their full cooperation and assistance during this project.

Lori Brooks

Lori Brooks, CPA, CIA, CGAP, CRMA
City Auditor

Attachment

c: Trey Yelverton, City Manager
Theron Bowman, Deputy City Manager
Jim Parajon, Deputy City Manager
Gilbert Perales, Deputy City Manager
Don Crowson, Fire Chief
Will Johnson, Police Chief

CJIS Policy Review
Table of Contents

Page

Executive Summary

At the request of the City Manager's Office, the City Auditor's Office conducted a review of a recent Criminal Justice Information Services (CJIS) security issue associated with the Computer Aided Dispatch System (CAD), Intergraph 9.3 software upgrade. The review was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives. The objectives of the review were to:

- Identify and review access and security requirements related to use of CJIS and requirements for reporting violations and other issues
- Determine if appropriate testing of the software update was performed, to ensure integrity/access issues were addressed prior to the go live date
- Determine the extent of the security issue and when it was first known
- Determine when, how and to whom the issue was first reported
- Determine what actions were taken to properly rectify the issue and when
- Determine if unauthorized Fire Department staff inappropriately accessed, viewed, shared and/or used CJIS information

The City Auditor's Office noted the following:

- Most Fire Department staff members do not have authorized access to CJIS information, do not have experience with CJIS, and have not received training related to CJIS.
- It appears there was no malicious intent on the part of Arlington Fire Department staff, related to the CJIS data exposure.
- There was no evidence of misuse of the exposed CJIS information by Arlington Fire Department staff.
- The Fire Chief immediately requested updated policies and procedures to ensure a similar situation would not occur in the future.
- Texas Department of Public Safety appears to be satisfied with the reporting of the data exposure and the subsequent corrective action taken by Dispatch Services.

The City Auditor's Office identified opportunities for improvement in the following areas:

- Improved communication between Arlington Police, Fire and Information Technology Departments related to security issues and resolution
- Expediting software error resolution, based on compliance and operational risk
- Detailed policies and procedures for CJIS compliance and administration
- Detailed documentation for software testing and error resolution status

Audit findings and recommendations are discussed in the Detailed Audit Findings section of this report.

Audit Scope and Methodology

The review was conducted in accordance with generally accepted government auditing standards. The following methodology was used in completing the audit:

- Interviewed Dispatch, Police, Fire, and Information Technology staff members who use the system and/or assisted in implementation
- Interviewed Texas Department of Public Safety (DPS) employees in charge of CJIS security
- Examined emails and other documentation pertaining to CAD 9.3 implementation, system testing and data exposure
- Examined a sample of calls for service where CJIS data was visible to Fire Department personnel
- Reviewed CJIS access for selected Fire and Dispatch Services staff

Background

The City Auditor's Office responded to a request by the Arlington City Manager's Office to review a CJIS security issue related to the CAD 9.3 software upgrade. The software was upgraded to the 9.3 version from the original 9.1 version on May 12, 2015.

Intergraph CAD Administration

Dispatch Services is responsible for the appropriate use and administration of the Intergraph CAD software. Dispatch Services is part of the Arlington Fire Department. The primary role of Dispatch Services is to receive 911 emergency calls and dispatch Police, Fire and Ambulance Services throughout the city. Dispatch Services has established a designated CAD team to manage the software. The team provides technical advice, training and testing of the software. They also interact with the vendor to troubleshoot the software. The CAD team also provides oversight and support of Mobile Data Computer (MDC) units used mainly by Fire Department personnel. In addition, during the 9.3 project upgrade the CAD team included a member of the Information Technology Department to assist with the build process and work with the vendor, as applicable. It is important to note that Dispatch Services job responsibilities have become increasingly more technical, resulting in a higher demand for additional technical expertise.

Security Issue

The City Manager's Office became aware that restricted CJIS data was visible to Arlington Fire Department personnel via their MDCs. Arlington Firefighters are not given CJIS clearance to access or view CJIS data. This data is restricted to only certain criminal justice personnel in the course of their duties. The authority to access and view the data requires a background clearance. Inappropriate, unauthorized use of CJIS data could subject the user to personal criminal penalties. The types of information available from the CJIS system include prior criminal histories, vehicle information, and insurance information, which are typically used by policing agencies during traffic stops or criminal investigations. Although Firefighters are not given CJIS access, the Fire Investigators, as commissioned peace officers, do have access. The City has an agreement (Texas

Law Enforcement Telecommunications System Agency/Equipment Agreement) between DPS and the Arlington Police Department, the local law enforcement agency. This agreement is signed by the Director of DPS and the Arlington Police Chief as the Agency Administrator. There is a Management Control Agreement, regarding CJIS, between the Arlington Police Department, Fire Department, Information Technology Department and the City Manager's Office.

Arlington Police, Fire, and Ambulance Services use the Intergraph CAD 9.3 software via their MDCs, while responding to calls for service. The Informer software installed on the MDC units enables the receipt of CJIS information. The Informer software was installed on both Police and Fire MDC units when the original Intergraph 9.1 software was implemented. Due to the use of a "hot swap program," whereby Fire MDC units can be swapped out and used by any Fire personnel, including the Fire Investigators, a decision was made to install the Informer software on all Fire MDCs.

The 9.1 version of the software included controls to prevent restricted crime data from being displayed in Fire Department MDC units. However, the software controls in the 9.3 version did not function as intended and displayed restricted data on Fire Department MDC units. It was eventually determined that this occurred when both Police and Fire responded to a call, and Police accessed CJIS data while Fire was on the call. Upon review, it was noted the joint response calls for service were mostly motor vehicle accidents, but included other calls as well.

Intergraph CAD Testing

The CAD team relied upon a Battalion Chief, assigned to field operations, to test the MDC features and functionality during the upgrade of the CAD software. Features and functionality of the Intergraph software (as opposed to MDCs) was tested by the CAD team during the upgrade. The test process for the 9.3 version of the software began in December 2014. The MDC testing process began in late February 2015. For the testing of MDCs, the assigned Battalion Chief utilized designated key staff members at various Fire Stations in the City to test the MDC units. The field personnel were expected to provide feedback about functionality of features (i.e. mapping) and any identified failures to the CAD team on a regular basis. The CAD team was then responsible to communicate with the software vendor to resolve any issues.

Notifications Related to Security Issue

Field personnel testing MDC units informed the CAD team via email in March 2015 that CJIS test data was visible on Fire MDCs. On May 17, 2015, after the software go live, a similar report regarding CJIS data exposure was made via email. Further, an email on June 6, 2015 included notification to Fire Command Staff. Additionally, according to interviews and communications with Fire staff members, Fire personnel (outside of the official MDC test team) verbally notified Command Staff of data exposures between go-live and mid-July 2015.

On July 23, 2015, at a Meet and Confer meeting with the Arlington Professional Firefighters Association, a member of the Fire Department noted that he could see CJIS returns on his MDC. Fire Command Staff, City Executive Management and the Police Chief attended the meeting. Although

Fire Command Staff had been aware of the security issue, they believed it had been rectified. The Arlington Police Chief was first made aware of the CJIS security issue at this meeting.

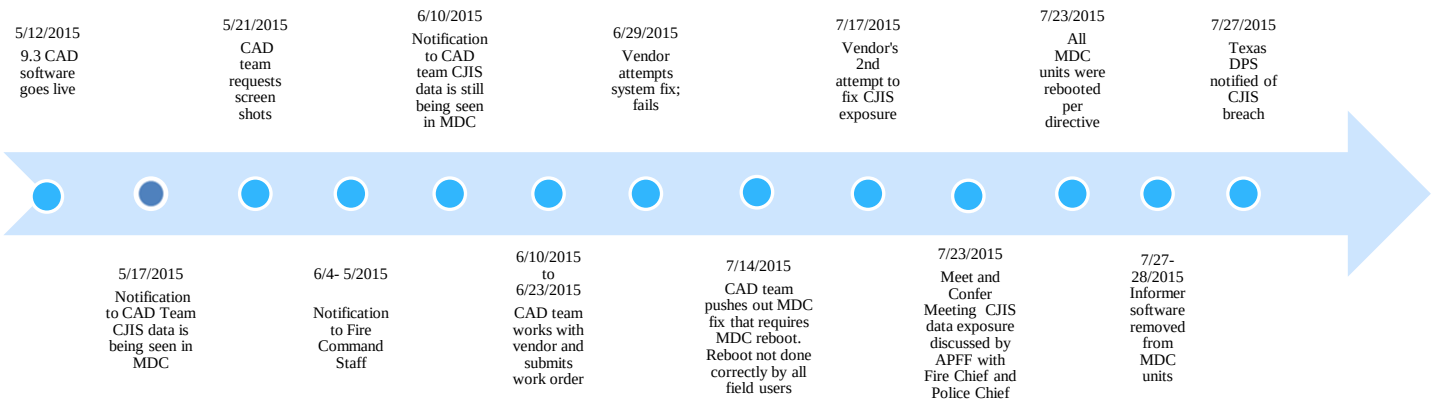
Corrective Action

On May 17, 2015, the Battalion Chief responsible for MDC testing notified the CAD team that CJIS data was visible on the Fire MDCs. As a result of this notification, on May 21, 2015, the CAD team requested that the Battalion Chief provide screen shots of the CJIS return. On June 23, 2015, the CAD team submitted a work order to Intergraph related to the CJIS data exposure. In response to this work order, Intergraph attempted a system fix on June 29, 2015; however, this did not correct the issue. On July 14, 2015, the CAD team created and pushed out an MDC fix that required an MDC reboot in order for the fix to take effect. The field users were not informed that a reboot was necessary to correct the CJIS security issue; therefore, the reboot was not performed correctly for all MDCs. It was assumed they would reboot their MDC's, per policy, as part of their daily routine; therefore, no additional instructions were communicated. According to Dispatch Services, this fix resolved the problem for those MDCs that were rebooted.

On July 17, 2015, Intergraph again attempted a system fix that would be vendor supported going forward. However, on July 23, 2015, at the Meet and Confer meeting, Fire Command Staff was made aware that the CJIS data was still visible on the MDCs. Immediately, Fire Command Staff ordered a mandatory reboot and verified that each MDC had been rebooted. Additionally, on July 27, 2015, the Informer software that allows access to CJIS data was removed from all Fire MDCs. This measure alone ensured that CJIS data would no longer be present and visible on the MDCs.

Timeline

The following is a timeline of events illustrating details regarding notification and corrective action related to the CJIS data exposure.



Additional Subsequent Data Exposure

A second data exposure was discovered on September 17, 2015. This event occurred following the corrective action initiated after the Meet and Confer meeting. The error was discovered during maintenance activity, when they switched over from the primary CAD server to the backup server. During the switch over, an MDC at Fire Station 7 displayed restricted CJIS data.

It was determined that the vendor patch previously applied to the primary server, to remedy the CJIS security issue, had not been applied to the backup server. Additionally, the Informer software had not been removed from that MDC unit. Removal of Informer software from all fire MDC units was ordered immediately following the Meet and Confer meeting in July 2015.

Extent of Exposure

Between May 12, 2015 and July 23, 2015 (time period during which known unauthorized data exposures occurred), there were a total of 1,574 calls for service, where both Fire and Police staff responded. It is important to note that although Fire personnel could see CJIS returns on their MDCs when inquiries were made by Police Officers or Dispatch while Fire was on the combined call, they did not have the ability to access the CJIS system and run criminal information. This requires access via credentials assigned by DPS. Fire personnel, other than Investigators, do not have these assigned credentials.

Detailed Audit Findings

Lack of Effective Communication

During interviews with Firefighters, Fire Command Staff, Dispatch Services Staff and others, it is apparent that communication between these parties, related to this issue, was untimely, incomplete and often non-existent. Pervasive communication issues were noted throughout the CJIS security incident. These include:

- The incident was not officially reported in writing to DPS immediately
- The Command Staff was not notified promptly or kept apprised of the situation
- The incident was not reported to the Police Chief
- There was no global communication to all Fire Department field users about the ongoing CJIS issue and the need to report exposures to the CAD team
- There was no specific communication to field users about the need to reboot the MDCs to ensure the software fix was applied
- There was incomplete communication between the Battalion Chief assigned to test the MDCs and the CAD team

Although verbal reporting and communication appears to have occurred sooner, a written incident report was not submitted to DPS until July 27, 2015. Additionally, while the security incident was known on May 17, 2015 following go-live, notification to Fire Command Staff was not made until

June 4, 2015. The Police Chief was not made aware of the issue until the Meet and Confer meeting on July 23, 2015.

Field personnel were neither notified there was an issue related to CJIS nor instructed about the data restrictions or asked to report any known exposures. Additionally, although remedial action to complete the software fix included the requirement of field personnel to reboot their MDC's, no specific communication was made to the field personnel. It was assumed they would reboot their MDC's as part of their daily routine; therefore, no additional instructions were communicated.

The Battalion Chief assigned to test the MDC's reported the data exposures to the CAD team; however, comprehensive, continued communication about the success/failure of remedial actions and any further data exposures was incomplete. This led to continued data exposure to Firefighters long after the situation was first discovered.

Recommendation:

1. ***The City Auditor's Office recommends that the Fire Chief establish appropriate protocols for effective communication between the CAD Team, Fire Command Staff, field personnel, Arlington Police Department and others outside the department as necessary.***

Lack of Timely Comprehensive Corrective Action

It is important to note that the ability to receive CJIS information on the Fire MDCs was accomplished through installation of the Informer software. Removal of Informer software was not considered until after the July 23, 2015 Meet and Confer meeting. Immediate removal of the software would have prevented any further unauthorized exposure. This option, however, was not considered earlier due to the use of a "hot swap" program described earlier in this report, whereby MDC units can be exchanged and used among all Fire personnel, including Fire Investigators who are authorized to access CJIS. In hind sight, this decision to install Informer on all Fire MDCs allowed the security breach to occur. Based on interviews with Police, Fire, and IT personnel, it is evident that the risks associated with this decision were not fully discussed and vetted by all pertinent parties.

Corrective action to resolve the CJIS data exposure issue was not managed in a comprehensive, expedited manner by the CAD team. Notification of unauthorized exposure to CJIS information with the Intergraph CAD 9.3 version was being reported as soon as five (5) days after the software upgrade go live date of May 12, 2015, and available documented reports from the field continued until June 10, 2015. During this time period, Dispatch Services used a Fire MDC for testing purposes and was unable to replicate the problem due to the circumstances necessary for the exposure to occur. Substantial resolution was not achieved until the end of July 2015.

Per the existing contract with the vendor, software errors should be prioritized based on current operational risks and entered into the work order management system. Corrective action is then initiated by the vendor and coordinated with the core CAD team for prompt resolution. Coordination includes testing of corrective action by the CAD team to ensure success of remedial action.

When the reports of data exposure began coming in to the CAD team, they requested that Fire personnel, responsible for field testing, provide actual printed evidence of CJIS data exposure, as this was requested by the vendor to evaluate the issue. According to Dispatch Services, the situation was discussed with Intergraph while representatives were on site, along with other issues. A work order was submitted to the vendor on June 23, 2015.

Per interviews with Dispatch Services, Intergraph CAD software issues related to unauthorized exposure to CJIS data was known as far back as when the CAD team visited the City of Tucson, AZ in September 2012. The City of Tucson uses the Intergraph system and shared an experience with unauthorized CJIS information exposure. Issues related to unauthorized exposure in the Arlington environment were also identified prior to go live of the 9.1 version of CAD software. These early errors in Arlington were corrected by the vendor prior to go live of the 9.1 version.

Even with prior knowledge of potential problems, the 9.3 version went live with the same issues. This was due in part to the fact that the CAD team had expected the vendor to carry over or apply the software controls put in place for the 9.1 version of software to the upgraded 9.3 version. However, it is not evident that effective testing was conducted to ensure these controls were carried over in the 9.3 upgrade. The initial work order to correct the data exposure in the 9.3 software upgrade occurred on June 23, 2015; approximately 6 weeks after the upgraded software went live. The initial corrective action by the vendor was implemented June 29, 2015, but it was not successful.

On July 14, 2015, the CAD team pushed out an MDC fix that required rebooting of the MDCs. The reboot requirement was not communicated officially to all Fire field personnel, and the remedial action did not take effect on MDC units that were not rebooted. According to interviews conducted with Fire management staff, an official communication related to the required reboot was not done because policy directs that staff should reboot their MDCs daily as part of their routine. According to Dispatch Services, this fix resolved the problem for those MDCs that were rebooted.

On July 17, 2015, Intergraph again attempted a system fix that would be vendor supported going forward. However, at the Meet and Confer meeting, Fire personnel informed Fire Command Staff that CJIS data was still visible on the MDCs.

Following the July 23, 2015 Meet and Confer meeting, Fire Command Staff ordered the reboot of all MDC units, under management supervision, and the removal of the Informer software from all Fire MDCs. However, as noted earlier, a second data exposure was discovered on September 17, 2015. The error was discovered during maintenance activity, when they switched over from the primary CAD server to the backup server. It should be noted that the incident was reported to Command Staff and DPS immediately.

The vendor patch previously applied to the primary server had not been applied to the backup server. During the switch over, an MDC at Fire Station 7 displayed restricted CJIS data. The Informer software had not been removed from that MDC unit. Because the Fire Department does not maintain a master inventory list with the location of all MDCs, neither Command Staff nor Dispatch Services ensured that all MDCs were collected and the software removed.

Recommendations:

2. ***The City Auditor's Office recommends that the Arlington Fire Chief require Dispatch Services to develop a compliance and risk based error resolution process for its CAD software, and to expedite error resolution based on operational risks.***
3. ***The City Auditor's Office recommends that the Arlington Fire Chief ensure the development and maintenance of an inventory of all Fire Department MDCs and their locations.***

Lack of Detailed Policies and Procedures for CJIS Compliance and Administration

Dispatch Services, a part of the Fire Department, follows the FBI CJIS Policy. However, there are no detailed internal policies and procedures, within the Fire Department, providing specific guidance and direction to Dispatch Services and other Fire Department staff, regarding CJIS compliance and administration. The City Auditor's Office identified the following areas that require specific guidance and direction:

- Definition of CJIS security exceptions and related reporting requirements
- Specific requirements related to method and timeliness of notification to DPS and City officials
- Assignment, identification and tracking of Fire Department MDC units
- Timely vendor resolution of CAD software issues, related to CJIS, based on priority
- Routine assessment of CAD compliance and operability, related to CJIS

Comprehensive policies and procedures should provide users with guidance on critical functions, related to meeting compliance, operational and contractual requirements. They should define exceptions and identify appropriate methodologies to follow in the event of a negative impact on operations.

According to Dispatch Services, a policy specific to CJIS compliance and administration does not exist within the Fire Department. Within the City of Arlington, the only internal polices related to CJIS compliance requirements are incorporated into Police General Orders, which include but are not limited to the following:

- Visitor and employee access to buildings where CJIS information is accessed/viewed, including the dispatch center where CAD software is in operation
- Computer terminal security
- Release of criminal history information

The lack of specific internal Fire Department policies and procedures, related to CJIS security requirements, contributed to the inconsistent reporting, response and follow up of the CJIS security issue, and the management of software testing and follow up activity, as well.

Following the July 2015 Meet and Confer meeting, the Arlington Fire Chief requested Command Staff develop updated policies and procedures related to CJIS security and management to include:

- Immediate reporting of security incidents
- Regular CJIS compliance status reporting
- Updated list of all personnel to include CJIS access status
- Inventory of all computers with CJIS access
- Updated training plans for employees related to CJIS
- Quality Assurance Program for CJIS policy compliance

Recommendation:

4. ***The City Auditor's Office recommends that the Arlington Fire Chief ensure that departmental policies and procedures are updated to include guidance and direction related to the above compliance and administrative issues.***

Lack of Adequate Software Testing Documentation

Inadequate documentation of testing for the Intergraph CAD 9.3 system resulted in a lack of clear evidence of the timing and nature of the tests conducted. Although documentation indicates testing occurred to ensure connectivity to CJIS, it is not evident that testing was based on other compliance requirements. Software testing was documented in a spreadsheet, which included minimal details and excluded critical information, such as the nature of the test, expected results, status of test failures, testing timeframe and approval of test results by management. It is not evident that system functionality that must meet specific compliance requirements, such as those related to CJIS, were prioritized and tested accordingly.

Generally accepted software test and documentation standards require maintaining documentation that can be interpreted easily, when a new system is implemented or upgraded. Adequate documentation provides evidence and support that system features required of the vendor are working as intended, and support operational requirements. A risk based test plan, a necessary tool when staffing resources are scarce, would ensure key compliance and operational system features are tested as required.

Testing of MDC functionality was delegated to Fire Department subject matter experts in the field, without specific test scripts or conditions under which to test. MDC testers did not report directly to Dispatch Management, which contributed to a lack of sufficient communication, follow up and documentation, related to MDC testing and CJIS related issues identified.

Incomplete test documentation made it difficult to determine test result status and what corrective action was taken by the vendor for test failures. Lack of details in the master test sheet also made it difficult to determine if follow up activity was necessary on any pending work orders.

Recommendation:

5. ***The City Auditor's Office recommends that for future software upgrades and enhancements, the Arlington Fire Chief require that detailed software test documentation is maintained.***

CITY OF ARLINGTON
CJIS POLICY REVIEW
MANAGEMENT RESPONSE AND ACTION PLAN

AUDIT RECOMMENDATION	CONCUR/DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE
1. ***The City Auditor's Office recommends that the Fire Chief establish appropriate protocols for effective communication between the CAD Team, Fire Command Staff, field personnel, Arlington Police Department and others outside the department as necessary.***	CONCUR	Procedures have been established to ensure thorough communication between all affected departments. The notification process has been utilized on several occasions during maintenance, updates and outages. We are in the process of writing this procedure into policy.	Dana Craig Jeremy Hensley Lupe Alba Rhonda Shipp Reps from other departments TBD	January 31, 2016
2. ***The City Auditor's Office recommends that the Arlington Fire Chief require Dispatch Services to develop a compliance and risk based error resolution process for its CAD software, and to expedite error resolution based on operational risks.***	CONCUR	The CAD team will work with stakeholders and the CAD vendor to develop the best tool. Dispatch Services has already implemented a revised notification process to ensure all affected parties are promptly informed.	Dana Craig Jeremy Hensley Lupe Alba Rhonda Shipp	May 31, 2016
3. ***The City Auditor's Office recommends that the Arlington Fire Chief ensure the development and maintenance of an inventory of all Fire Department MDCs and their location.***	CONCUR	Dispatch Services has developed a process to document maintenance for all MDCs. It will be up to the Police and Fire Departments to maintain inventory on the exact location of their equipment. There is software available through NetMotion called Locality that can be utilized to track assets, geo-locate and remotely troubleshoot issues.	Jim Self Jaime Ayala Jeremy Hensley Lupe Alba	Dispatch portion already implemented. May 2016 for remaining items

AUDIT RECOMMENDATION	CONCUR/DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE
4. ***The City Auditor's Office recommends that the Arlington Fire Chief ensure that departmental policies and procedures are updated to include guidance and direction related to the above compliance and administrative issues.***	CONCUR	Dispatch Services already complies with the CJIS policy issued by the FBI. We have started developing a departmental CJIS policy outlining all stakeholder roles and responsibilities for complying with CJIS.	Dana Craig Jeremy Hensley Rhonda Shipp Sha Curtis Sheila Powers	February 27, 2016
5. ***The City Auditor's Office recommends that for future software upgrades and enhancements, the Arlington Fire Chief require that detailed software test documentation is maintained.***	CONCUR	The CAD team will research various testing methodology to ensure proper documentation is maintained. We will also reach out to the CAD vendor and other public safety communications center for guidance.	Dana Craig Jeremy Hensley Lupe Alba Rhonda Shipp	January 31, 2016