

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



**Executive Summary Concerning the Results
of an Office of the Inspector General Investigation
Into Misconduct Violation by an Employee of the
District of Columbia Office of Unified Communications**

2009-0111(S)

INVESTIGATIVE SYNOPSIS

The District of Columbia Office of the Inspector General (OIG) investigated allegations that an Office of Unified Communications (OUC) Customer Service Supervisor has access to the National Crime Information Center (NCIC) and the Washington Area Law Enforcement Systems (WALES), even though he has a criminal history.

During the investigation, OIG investigators interviewed the Metropolitan Police Department (MPD) NCIC and WALES Program Manager, who also is the District's Criminal Justice Information Services (CJIS) Systems Officer (CSO) (District CSO), and the CJIS Management and Program Analyst (CJIS Program Analyst). OIG investigators also reviewed the security policies that govern access to NCIC and WALES. In addition, OIG investigators interviewed the Customer Service Supervisor and reviewed his criminal history, Official Personnel File, and agency personnel file.

I. The Customer Service Supervisor

The OIG investigation revealed that the Customer Service Supervisor pled guilty to a Maryland misdemeanor in 1995 and received probation before judgment, which ended in June 1997. He also was arrested in the District in 1995 and charged with a felony, to which he pled guilty, and was convicted in 1997.

The Customer Service Supervisor's OUC agency personnel file and Official Personnel File revealed that he has been employed with the District government since 2000. He initially applied for District employment by submitting his resumé, and OIG investigators did not find any documents pertaining to his initial hiring on which he was required to disclose his conviction.

In September 2004, the Customer Service Supervisor submitted a D.C. Employment Application (DC 2000) to the D.C. Department of Human Resources, which he signed on September 7, 2004. He failed to disclose his 1997 felony conviction on the September 7, 2004, DC 2000. Specifically, the Customer Service Supervisor answered "No" to the question of whether he had been convicted of a felony within 10 years.

In his interview, the Customer Service Supervisor told OIG investigators that he had two arrests, one resulting in a felony conviction and another resulting in a misdemeanor conviction. He also told OIG investigators that he understood that his 1997 plea had resulted in a felony conviction; however, when he filled out the DC 2000, he could not remember the date of his felony conviction and thought that it had occurred outside the 10-year time period.¹

II. Access to NCIC and WALES

OIG investigators learned that NCIC, the United States central database for tracking crime-related information, is maintained by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (CJIS). It is interlinked with similar systems maintained by each state. WALES, the District's central database for tracking crime-related information, is maintained by MPD and interlinked with NCIC. Access to NCIC is governed by the CJIS Security Policy (February 2011)².

The CJIS Security Policy's essential premise, as set forth in Section 1.1, is to provide "appropriate controls to protect criminal justice information (CJI) from creation to dissemination; whether at rest or in transit." The policy provides the minimum set of physical and personnel security requirements for access to FBI and CJIS systems (NCIC) and to protect and safeguard CJI. The policy allows any CJIS Systems Agency³ and all user agencies to develop more detailed or stricter security standards, guidelines, and procedures.

A. CJIS Physical Security Requirements

The CJIS Security Policy requires the implementation of physical protection policies and procedures to ensure CJI and information system hardware, software, and media are physically protected through access control measures sufficient to prevent unauthorized access and viewing.

OIG investigators toured OUC's Unified Communication Center (UCC) and observed that both 911 and 311 are co-located in a large space that lacks physical barriers to separate the two operations. The room's layout provides 311 personnel with unrestricted physical and visual access to the 911 area where computer terminals with access to NCIC, WALES, and other sensitive law enforcement information are located.

OIG investigators described the UCC design and layout to the CJIS Program Analyst, who is the designated CJIS Auditor for MPD and the District's NCIC user agencies. She told OIG investigators that the physical layout complies with CJIS physical security

¹ The OIG investigation found no evidence that OUC was aware of the Customer Service Supervisor's conviction.

² Access to WALES is not governed by the CJIS Security Policy. Because MPD accesses WALES and NCIC through the same computers, however, MPD follows the CJIS Security Policy for both systems.

³ MPD serves as the CJIS Systems Agency for the District and provides District government agencies with access to the various systems managed by CJIS.

requirements because the operations center is in a secure area of the building. She also told OIG investigators that anyone with unescorted access to this area must comply with CJIS personnel security requirements.

B. CJIS Personnel Security Requirements

The CJIS Security Policy requires the screening of all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process, or transmit unencrypted CJI. To verify the identification of personnel, the policy requires a state of residency and a national fingerprint-based record check for all personnel who have “direct access”⁴ to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

The policy also imposes certain access restrictions based on a person’s criminal history. A person with a felony conviction of any kind shall be denied access to CJI. A user, however, may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

In addition, if a record of any other kind exists, or if the person appears to be a fugitive or to have an arrest history without a conviction, access to CJI shall not be granted until the CSO reviews the matter to determine if access to CJI is appropriate. Finally, if a person who already has access to CJI is subsequently arrested and/or convicted, the CSO is required to determine if continued access to CJI is appropriate. Where the CSO determines that access to CJI would not be in the public interest, access to NCIC and WALES shall be denied and the user agency shall be notified in writing of the denial. Written notification is not required when access is granted because the systems access itself serves as notification of approval.

The CJIS Security Policy requires that support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas, submit to a state of residency and a national fingerprint-based record check, unless they are escorted by authorized personnel⁵ at all times. The criminal history restrictions do not apply. According to the CJIS Program Analyst, even if an individual has a criminal record, a CSO review is not necessary unless the person is applying for direct systems access.

⁴ According to Appendix A of the policy, “direct access” means having the authority to access systems managed by CJIS, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency, and having the authority to query or update national databases maintained by CJIS including national queries and updates automatically or manually generated by the CJIS Systems Agency.

⁵ According to Appendix A of the policy, an “Authorized User/Personnel” is an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

The District CSO told OIG investigators that MPD follows the CJIS Security Policy when granting access to NCIC and WALES. She explained that generally MPD considers people with misdemeanor convictions or arrests without convictions that occurred more than 10 years prior to their request for access as eligible for direct system access. The District CSO also told OIG investigators that the security policy restrictions do not apply to those who supervise and manage employees with direct system access, as long as they themselves do not have direct system access.

In addition, the District CSO told OIG investigators that her NCIC and WALES certification and recertification processes do not involve background or record checks. OUC is responsible for conducting the required background and record checks and notifying her if an applicant for direct system access has a criminal history. OUC also is required to notify her when there is a change in the criminal history status of an OUC employee with direct system access, such as a new arrest or conviction after direct system access was granted. If OUC does not notify her of a change in criminal history status, she has no way of knowing that a criminal history review is needed. According to the District CSO, in the 10 years she has been the District's CSO, OUC never has requested a review of any employee's criminal history when the employee applied for direct system access.

III. Other OUC Employees with Criminal Histories

During the investigation, OIG investigators learned that in addition to the Customer Service Supervisor, 13 OUC employees had criminal histories. OIG investigators reviewed NCIC criminal history reports for these employees.

A. 911 Operators

Six OUC employees with criminal histories were assigned to 911 operations. Of those, three were 911 dispatchers who had direct access to NCIC and WALES and no felony conviction. (One of those 911 dispatchers had a 1989 felony arrest without conviction, one 911 dispatcher had a 2003 misdemeanor conviction⁶, and one 911 dispatcher had a 2008 felony arrest without conviction). OUC never applied for NCIC and WALES access for these three dispatchers because each had been granted access while employed with MPD and maintained that access when they became employees of the newly created OUC in 2004. OUC, however, should have notified MPD of the change in the third dispatcher's criminal history when that dispatcher was arrested in 2008, because that dispatcher had direct system access. Although OUC failed to make the proper notification to MPD at that time, OUC placed the employee on suspension following the employee's arrest. The employee remained on suspension until the charges were resolved without a conviction.

⁶ The OIG investigation could not determine whether the District CSO had reviewed the circumstances surrounding the arrests of these two employees in 1989 and 2003, respectively, and cleared them for continued systems access, because MPD does not maintain records of CSO approvals.

The remaining three 911 employees identified as having criminal histories were supervisors who did not have direct access to NCIC and WALES. Therefore, OUC was required only to ensure that they were submitted to a state of residency and a national fingerprint-based record check. The CJIS security restrictions regarding criminal history did not apply to these three 911 operations employees.

B. 311 Operators

The Customer Service Supervisor told OIG investigators that he was assigned to OUC's transcription center where he managed the transcription and production of recordings of radio transmissions and 911 calls. He neither had direct systems access to NCIC and WALES, nor directly supervised anyone with access.

In addition to the Customer Service Supervisor, seven other OUC employees assigned to 311 operations had criminal histories, but did not have direct access to NCIC and WALES. They were required only to submit to a state of residency and a national fingerprint-based record check. The CJIS security restrictions regarding criminal history did not apply to these eight OUC operations employees.

FINDINGS AND CONCLUSIONS

The OIG investigation determined that none of the 14 employees, including the Customer Service Supervisor, had criminal histories that violated CJIS security restrictions. With the exception of failing to notify the District CSO of the 911 dispatcher's 2008 arrest, OIG investigators found no evidence that OUC violated the CJIS Security Policy.

The OIG referred the matter of the Customer Service Supervisor's false statement to the United States Attorney's Office for the District of Columbia, which declined prosecution.

The Customer Service Supervisor failed to disclose a 1997 felony conviction on his DC 2000, despite being required to do so. Accordingly, the investigation has **substantiated** that the Customer Service Supervisor violated DPM § 1603.3 (c) (Knowing or negligent material misrepresentation on an employment application); § 1803.1(a) (6) (Affecting adversely the confidence of the public in the integrity of government).

For the remaining 13 OUC employees with criminal histories, the OIG investigation did not find any CJIS Security Policy violations. The OIG investigation found that OUC failed to notify MPD of the 2008 felony arrest of an active 911 operations employee who had direct systems access. If it had done so, the District CSO could have conducted a review to determine whether continued access to the NCIC and WALES databases was appropriate.

Finally, although the OIG investigation did not reveal violations of CJIS security policies, the OIG notes that the CJIS Security Policy sets minimum acceptable security standards and does not prohibit an agency from setting more stringent standards. The OIG believes

that more stringent security standards than those required are appropriate because additional, stricter security policies would better safeguard the information contained in the NCIC and WALES databases from unauthorized access and viewing, inappropriate use, and unnecessary dissemination.

RECOMMENDATIONS

Based on the results of this investigation, the OIG recommends that OUC:

- Address the Customer Service Supervisor's conduct with appropriate administrative action;
- Ensure that all OUC employees have had the required state of residency and national fingerprint-based record check conducted by MPD;
- Coordinate with MPD to ensure that both MPD and OUC maintain a record of requests for criminal history review of OUC NCIC applicants, indicating the identity of the applicant, the identity of the District CSO who performed the review, the resulting decision, and the date of the decision;
- Consider separating the 911 Emergency Operations area from the 311 Non-Emergency Operations area with a physical barrier, and restrict access to the 911 area to personnel assigned to 911 Emergency Operations only; and
- Assign only managers and supervisors who do not have a criminal history to the 911 Emergency Operations. Alternatively, if a manager or supervisor has an arrest history (with or without conviction) for a felony or misdemeanor, request a review by the District CSO to determine whether supervision of personnel having NCIC and WALES access is appropriate.

July 12, 2011