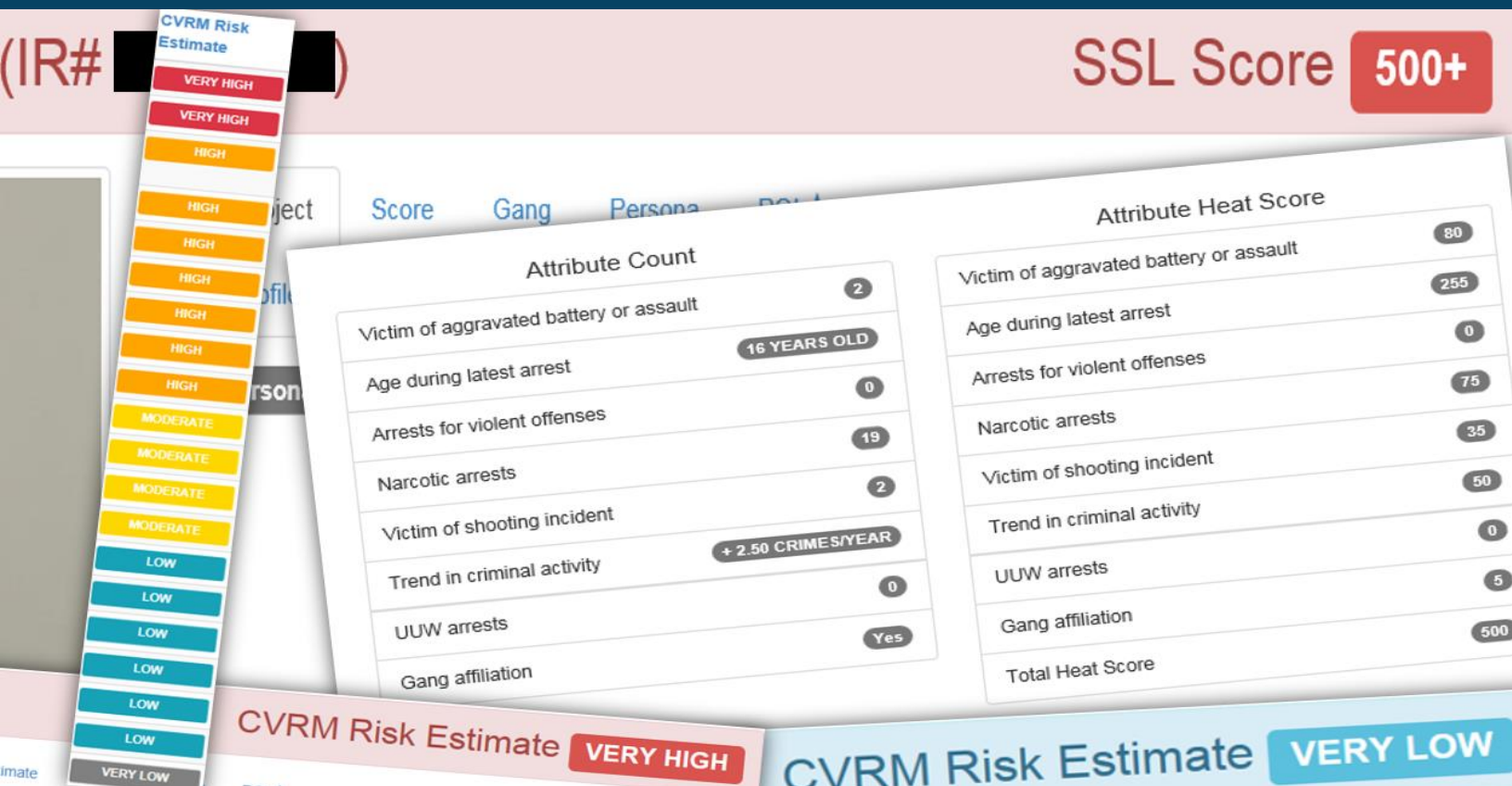


JANUARY 2020

CITY OF CHICAGO OFFICE OF INSPECTOR GENERAL

ADVISORY CONCERNING THE CHICAGO POLICE DEPARTMENT'S PREDICTIVE RISK MODELS





JOSEPH M. FERGUSON
INSPECTOR GENERAL

CITY OF CHICAGO
OFFICE OF INSPECTOR GENERAL
740 NORTH SEDGWICK STREET, SUITE 200
CHICAGO, ILLINOIS 60654
TELEPHONE: (773) 478-7799
FAX: (773) 478-3949

VIA ELECTRONIC MAIL

Charlie Beck
Interim Superintendent
Chicago Police Department
3510 South Michigan Avenue
Chicago, Illinois 60653

Re: The Chicago Police Department's Former Predictive Risk Models

The Office of Inspector General (OIG) conducted a review of the Chicago Police Department's (CPD or the "Department") risk models known as the Strategic Subject List (SSL) and Crime and Victimization Risk Model (CVRM). CPD received \$3.8 million in federal grants to develop these models, which were designed to predict the likelihood an individual would become a "party to violence" (PTV), i.e. the victim or offender in a shooting. The results of SSL were known as "risk scores" while CVRM produced "risk tiers." In August 2019, CPD informed OIG that it intended to decommission its PTV risk model program and did so on November 1, 2019 (although the grant period ended on September 30, 2019). The purpose of this advisory is to assess lessons learned and provide recommendations for future implementation of PTV risk models.

I. BACKGROUND

The Chicago Police Department began using a series of risk models to predict PTV individuals in 2012. The first five PTV risk models were iterations of SSL, while the sixth and most recent version was CVRM. Both models analyzed individuals' attributes to predict their likelihood of becoming a PTV over the next 18 months.

A research team from the Illinois Institute of Technology (IIT) created the six versions of the risk models and calculated the scores and tiers using deidentified data it received from CPD's Information Services Division (ISD). After receiving IIT's calculations, ISD in turn reidentified the data to map scores and tiers to specific individuals. CPD contracted the RAND Corporation (RAND), a nonprofit global policy think tank, to evaluate Versions 1, 5, and 6 of the model. The attributes used by the models to generate risk scores and tiers were,¹

- incidents as shooting victim,
- age at latest arrest,

¹ These are the attributes used by Versions 5 and 6 of the model, i.e. the versions evaluated by OIG.

- incidents as victim of aggravated battery or assault,
- trend in involvement in crime incidents,
- arrests for unauthorized use of a weapon,
- violent incidents as arrestee,
- narcotics arrests (SSL Version 5 only), and
- gang affiliation (SSL Version 5 only).

In theory, the higher the risk score or tier, the greater the risk of becoming PTV.

CPD collated individuals' risk scores and tiers, along with additional information, into a single dashboard, accessible by all CPD personnel. Additionally, CPD included risk scores and tiers in Caboodle, a geospatial mapping application used to map criminal activity.

A. INDIVIDUALS WHO RECEIVED A RISK SCORE OR TIER

Every individual arrested at least once within a four-year time period prior to IIT's calculation—regardless of whether they had a history of violence—received a risk score or risk tier.² As of July 2018, 399,412 individuals had an SSL risk score and as of March 2019, 313,513 individuals had a CVRM risk tier.³

Individuals who were victims of crimes, but never arrested, did not receive a risk score or tier. According to CPD, this was because victims—unlike arrestees—do not have a unique identifier, such an Individual Record (IR) number,⁴ on record. This means that an individual arrested for a non-violent misdemeanor (for example, certain instances of driving over the speed limit), might have been assigned a risk score or tier while a victim of a gunshot wound (who was never arrested) would not have been included in the model.

B. CPD'S USE OF RISK SCORES AND TIERS

Over the course of the PTV program, CPD used its PTV risk models in several ways, including:

- Custom Notification Program: CPD used the prediction model to help inform referrals to its Custom Notification Program, designed to identify at-risk individuals and connect

² The demographic breakdown of individuals with risk scores and tiers actually reflects the demographic breakdown of arrests in Chicago.

³ These numbers are higher than publicly available datasets for SSL and CVRM on the City of Chicago's Data Portal and CPD's Violence Reduction Strategy webpage, respectively. Publicly available datasets do not include every individual who received a risk factor.

⁴ Every individual who has been arrested and fingerprinted by CPD is assigned an IR number. The IR number identifies an individual, not an arrest. Therefore, if an individual is arrested multiple times, their IR number will have multiple arrests associated with it.

them to social support services.⁵ (According to CPD directives, the risk scores or tiers were among several factors guiding referrals to this program);⁶

- Targeted Repeat-Offender Apprehension and Prosecution (T.R.A.P) Program: According to CPD's Special Order S10-06, T.R.A.P. "allows the Department and the State's Attorney's Office to work together to identify repeat offenders with the high propensity toward violent, gang-related crime." The program "focuse[s] on enhanced prosecution to detain, convict, and incarcerate these offenders."⁷ District commanders may have used an individual's SSL score as one of ten potential criteria in determining eligibility for the program; and
- Gang Violence Reduction Strategy (GVRS): CPD's General Order G10-01 describes GVRS as "comprised of multiple components: information gathering, analysis, dissemination of intelligence, linking of gangs to their factions, social network mapping, and a variety of mission-specific operations focused on targeted gang members and their associates."⁸ CPD stated that SSL was one of four "technical components" of GVRS.⁹

Additionally, beginning in March 2015, CPD began referring to SSL risk scores in the narrative sections of arrest reports (i.e. either including an individual's SSL score or noting that the arrestee did not have an SSL score).

C. SCOPE AND METHODOLOGY

OIG reviewed Version 5 and Version 6 of CPD's PTV risk models (i.e. the last version of SSL and CVRM).

OIG analyzed data from the City of Chicago's Data Portal, CPD's internal dashboards, and arrest reports. Additionally, OIG interviewed personnel from CPD, RAND, and Cook County Sheriff's Office, as well as Miles Wernick, Ph.D., from IIT, and Cathy O'Neil, author of *Weapons of Math Destruction*.

⁵ CPD Violence Reduction Strategy, accessed October 16, 2019, <https://home.chicagopolice.org/violence-reduction-strategy-vrs/>.

⁶ CPD Special Order S09-11, accessed August 21, 2019, <http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html>, and CPD Special Order S10-05, accessed August 21, 2019, <http://directives.chicagopolice.org/directives/data/a7a57bf0-1456faf9-bfa14-570a-a2deebf33c56ae59.html>.

⁷ CPD Special Order S10-06 "Targeted Repeat-Offender Apprehension and Prosecution (T.R.A.P.) Program", accessed August 21, 2019, <http://directives.chicagopolice.org/directives/data/a7a57b38-14eabf49-88714-eabf-585e2775112f376d.html>.

⁸ CPD General Order G10-01, accessed October 16, 2019, <http://directives.chicagopolice.org/directives/data/a7a57bf0-136d1d31-16513-6d1d-382b311ddf65fd3a.pdf>.

⁹ Other components were the Gang Audit, the District Intelligence Bulletin, and the Major Incident Notification application.

OIG also reviewed: CPD training material, policies, and directives; emails sent from CPD's Office of the Superintendent to the Mayor's Office; examples of Cook County Sheriff's Office's Chicago Initiative summaries; and federal grants for CPD's PTV risk models from 2009 to 2015.

II. GENERAL AREAS OF CONCERN IDENTIFIED IN THE PTV RISK MODEL PROGRAM

1. Risk scores and tiers were unreliable.
2. CPD did not properly train sworn personnel to use PTV risk models.
3. CPD lacked controls for internal and external access to and use of PTV risk scores and tiers.
4. Interventions influenced by CPD's PTV risk models may have attached negative consequences to arrests which did not result in convictions.
5. Neither CPD nor the RAND corporation evaluated Versions 2 through 5 of CPD's PTV risk models.
6. CPD did not develop a plan to sustain its PTV models.

III. RECOMMENDATIONS FOR ENSURING THE PTV RISK MODEL PROGRAM HAS BEEN PROPERLY DECOMMISSIONED

To properly decommission the program, OIG recommends that the Department,

1. appropriately revise its orders and directives to remove language referencing SSL and CVRM,
2. remove risk scores and tiers from CPD databases,
3. ensure all appropriate CPD personnel, including commanders and district intelligence officers (DIOs), are informed about the discontinuation of PTV risk models,
4. ensure external agencies no longer have access to risk scores or tiers, including any indirect means (e.g. email updates), and
5. determine whether other methods employed by officers are empirically based and can accurately predict individuals at risk of becoming PTV.

IV. RECOMMENDATIONS FOR FUTURE PTV PROGRAMS

Although CPD has decommissioned its recent PTV risk models, the Department stated that it may develop programs in the future which use data to help predict PTV individuals. Furthermore, CPD intended to use its PTV risk models as examples for other jurisdictions as part of the national discourse on predictive policing. OIG provides the following findings and recommendations to CPD and any other jurisdiction considering the use of data to predict PTV individuals.

A. CLEAN AND VET DATA AND DEVELOP PROTOCOLS TO REGULARLY UPDATE PTV-RELATED INFORMATION

CPD's risk scores and tiers were unreliable as they were not updated regularly and the quality of the data was, in certain respects, poor.¹⁰ Until CVRM was launched on January 9, 2019, SSL scores had not been updated since August 2016, resulting in scores which were static for nearly two and a half years. Specifically, CPD used and disseminated information that,

1. retained risk scores and tiers for individuals who were not arrested again within the four years following IIT's calculation,
2. did not assess the risks of individuals who were arrested after the risk scores and tiers were last calculated, and
3. did not account for additional activity that could impact individuals' risk scores and tiers.

Additionally, OIG observed several problems in CPD data, including missing age at latest arrest, criminal activity occurring after death dates, and conflicting Unlawful Use of a Weapon (UUW) data.¹¹ Although these data quality issues impacted a small percentage of the total population of individuals with a risk score or tier, the scores or tiers for such individuals may not have been correctly calculated. Specifically, age at latest arrest may have significantly impacted an individual's risk score or tier, particularly given that age was inversely related to risk score or tier, i.e. higher scores and tiers were associated with younger ages.

For any programs using data to predict PTV individuals, CPD and partner entities should assess data quality to ensure its reliability, such as:

- cleaning and vetting data to ensure it is accurate and complete, and
- developing protocols to continuously update information to ensure data is current.

B. CONDUCT TRAINING IN A TIMELY MANNER WITH UP-TO-DATE MATERIAL

CPD did not update training materials on the use of its PTV risk models. The only training material developed for CPD command staff was created for Version 3 of SSL and stated that the variables used to calculate SSL scores included the number of times an individual was co-arrested with another PTV individual, which, by Version 5, was already inaccurate. Additionally, CPD did not ensure that commanders received training regarding PTV risk models. OIG spoke with two commanders who were unaware of any formal training.

¹⁰ Here OIG uses reliability not in the technical, statistical validation sense but rather in the broader common parlance of adequate basis for operational use.

¹¹ Both SSL and CVRM datasets offered UUW information for two time periods: four years and ten years. OIG's analysis revealed that the data might show a person having more UUW incidents in a four-year period than a ten-year period.

Without proper training or guidance, district commanders may not have understood the purpose of PTV predictive models or how to apply risk scores or tiers, and may have had incomplete, outdated, or inconsistent information about what the outputs from these models meant. For example, of the 398,684 individuals who had an SSL score in Version 5 of the model, 16.3% (or 64,947) were identified as confirmed gang members. However, one district commander estimated that about 95% of the individuals who had an SSL score were gang members or associates, while a DIO stated that everyone who has an SSL score is a gang member. In another example, several CPD personnel, including a bureau chief and district commanders, stated that PTV models were intended only to predict PTV individuals for the Custom Notification Program; however, T.R.A.P. and GVRs directives discuss the application of the model as well.¹²

CPD should conduct training in a timely manner with up-to-date material to ensure correct and consistent understanding and use of predictive data.

C. CREATE POLICY DICTATING THE INTENDED PURPOSE AND ALLOWED USES OF PTV INFORMATION AND MONITOR THE USE OF INFORMATION

CPD allowed all sworn personnel to access risk scores or tiers via its internal dashboards, regardless of whether their duties were related to any of the uses outlined in various directives, thereby increasing the likelihood of misuse.¹³ CPD did not attempt to mitigate the risk of unintended usage of risk scores and tiers by monitoring internal access to, and application of, this information; there was no supervisory protocol in place to support compliance with the tool's intended use.

Additionally, CPD personnel, including senior staff from the Bureau of Technical Services and members of ISD, told OIG that no external agencies had access to the SSL dashboard or SSL risk scores; this proved to be inaccurate. Risk scores and tiers were shared with the following external entities:

1. Cook County Sheriff's Office (CCSO): In July 2015, CPD signed a data sharing agreement with CCSO. Giving CCSO access to SSL scores. CCSO used SSL for its Sheriff's Anti-Violence Effort (SAVE)¹⁴ and Chicago Initiative¹⁵ programs.

¹² Possibly exacerbating this confusion is CPD not updating all directives to reflect the change from SSL to CVRM. As of August 9, 2019, CPD's Special Order S10-05 "Custom Notifications in Chicago" and Special Order S10-06 "Targeted Repeat-Offender Apprehension and Prosecution (T.R.A.P.) Program" still referred to SSL, although CPD had launched CVRM on January 9, 2019.

¹³ Additionally, CPD may have exacerbated the effects of this lenient access policy by not updating its directives and not offering updated trainings to relevant personnel (see section III.B).

¹⁴ SAVE is a voluntary program which engages with individuals in custody who are likely to experience violence, through methods such as conflict resolution and anger management.

¹⁵ In April 2019, CCSO described the Chicago Initiative to OIG as focused anti-violence efforts supporting the City of Chicago in District 6 as well as other parts of the City.

2. The Mayor's Office: CPD's Office of the Superintendent sends the Mayor's Office email briefings on the previous day's "murders and shootings," if applicable.¹⁶ The briefings may include a description of the event and, as of January 8, 2019, sometimes included whether or not the victim or offender had an SSL score.
3. The Cook County State's Attorney's Office (CCSAO): CPD sometimes sent records to CCSAO which included defendants' risk scores or tiers.

Additionally, risk scores and tiers were available to external agencies who had access to arrest reports.

Personnel from external agencies stated they did not receive guidelines on how to use risk scores and tiers. CPD also did not monitor the use of risk scores or tiers by external agencies, making misapplication of this information more likely.

CPD should create a policy delineating the intended purpose and permissible uses of PTV risk information and monitor its use. CPD should establish the necessary controls to guide and monitor internal and external use of information. To do so it should,

- develop and distribute protocols guiding the use of information,
- grant access to this information on an as-needed basis,
- inventory which external entities have access to predictive information, whether directly (e.g. a notification sent for the purpose of sharing related information) or indirectly (e.g. an arrest report to which it already has access), and
- monitor the use of this information.

D. CONSIDER ALL RELEVANT DATA TO PREDICT AND INTERVENE WITH INDIVIDUALS AT RISK OF BECOMING PTV

The fact that CPD's models generated PTV scores or tiers for all individuals arrested, including those not necessarily convicted, may have resulted in interventions which effectively punished individuals for criminal acts for which they had not been convicted. According to Special Order S10-05, individuals who received a custom notification as a result of a PTV risk score or tier, regardless of whether they were convicted, may have been subject to harsher charging decisions on subsequent arrests.¹⁷

In addition to these potentially high-impact consequences, failing to consider whether an individual was actually convicted may have yielded inaccurate data. Several of the attributes determining a risk score or tier were related to arrests, and assumed that the arrestee did in fact

¹⁶ OIG received copies of the emails sent from the Superintendent's Office to the Mayor's Office from September 26, 2018 to June 5, 2019.

¹⁷ Risk score and tiers were not the only source of referrals to the Custom Notification Program, which continues after the decommission of the risk models. This means that individuals referred to the Custom Notification Program by means other than risk score or tier may still be subject to the harsher charging conditions outlined in the directive.

commit the crime for which they were arrested. If an individual was released without charges or was charged and acquitted, or if the charges were dismissed, that individual would have had a risk score or tier which factored in an offense which they were never found to have committed; for those individuals, differentiating between arrests and convictions would have ultimately changed (i.e. lowered, or even eliminated) the risk score or tier.

CPD should consider all available relevant data to predict and intervene with individuals at risk of becoming PTV. To ensure that the rights of individuals are appropriately protected, whenever the potential for negative consequences is possible, CPD should thoughtfully distinguish between arrests and convictions. Recognizing that court processes are lengthy and that waiting for final disposition of criminal charges could lead to a delay in producing timely risk scores or tiers, PTV prediction tools should nonetheless account for an arrest with a conviction and an arrest without a conviction differently (as well as whether the individual who was arrested was ever charged in the first place).¹⁸ Protocol should guide interventions and should consider whether a score indicates likelihood to become a victim, offender, or both.

E. CONTINUOUSLY EVALUATE THE ACCURACY AND EFFICACY OF PREDICTIVE POLICING PROGRAMS

Neither CPD nor RAND (which was periodically tasked with evaluating CPD's PTV risk models) evaluated Versions 2 through 5 of the models. An extension for CPD's 2015 federal funding noted, "Grant funds are to be used to conduct the necessary quantitative evaluation of the improved Strategic Subjects [*sic*] (SSL) software models and interventions (Model SSL v5 and Model SSL v6) that are created by IIT." RAND had evaluated Version 1 of CPD's PTV risk model; however, upon publication of the report, CPD announced that it was already using Version 5.

CPD should continuously evaluate the accuracy and efficacy of predictive policing programs. Evaluations should be timely so that the results can be used to improve program performance, and changes to data models and their application should be data-driven to ensure maximum positive impact on predictive policing.

F. DEVELOP PLANS AND SECURE RESOURCES TO ENSURE THE SUSTAINABILITY OF SUCH PROGRAMS

CPD's federal grant funding for the PTV program was set to end in September 2019, which included a one-year extension. As late as January 2019, CPD had not established plans for how it would sustain the model once its federal funding and partnership with IIT ended. In August 2019, when CPD informed OIG of its intention to decommission the PTV risk model program, the Department had not received the algorithmic model from IIT, a necessary step for continuing the

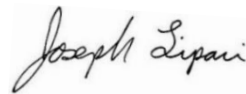
¹⁸ OIG does not offer a view on whether arrest alone is a predictor of PTV and therefore the recommendation is not meant to indicate *who* should be assessed for PTV risk, but rather to suggest measures to ensure that the rights of those who are assessed are protected.

program without IIT as a partner.¹⁹ Ensuring sustainability for a program such as this one would have included planning for technology, personnel, expertise, and funding. Because CPD never created a sustainable plan, OIG was unable to assess what resources CPD would have needed to support the continued use of risk models.

Upon receiving external funding to develop or implement a program using data to predict PTV individuals, CPD should develop a plan to ensure program sustainability and secure resources to support the program's existence beyond the immediate funding period. Sustainability planning should begin at the outset and be considered throughout life of the program. Sustainability plans help programs identify funding sources, so that when one source is exhausted, others can fill the gap.²⁰

We thank CPD for their cooperation in explaining risk models and providing requested documentation.

Respectfully,



Joseph L. Lipari
Deputy Inspector General, Public Safety
City of Chicago

CC: Dana O'Malley, General Counsel, Chicago Police Department
Christopher Taliaferro, Alderman, Chicago City Council
Susan Lee, Deputy Mayor of Public Safety, City of Chicago
Maurice Classen, Chief of Staff, Office of the Mayor

¹⁹ On November 21, 2019, CPD informed OIG that they expect to receive the algorithm the following week.

²⁰ Breem, Patricia, "Sustaining Evidenced-Based Practices. Justice, Research, and Statistics Association," 2015, p. 5 accessed October 8, 2019, http://www.irsa.org/projects/ebp_briefing_paper3.pdf.

MISSION

The City of Chicago Office of Inspector General (OIG) is an independent, nonpartisan oversight agency whose mission is to promote economy, efficiency, effectiveness, and integrity in the administration of programs and operations of City government. OIG achieves this mission through,

- administrative and criminal investigations by its Investigations Section;
- performance audits of City programs and operations by its Audit and Program Review Section;
- inspections, evaluations and reviews of City police and police accountability programs, operations, and policies by its Public Safety Section; and
- compliance audit and monitoring of City hiring and employment activities by its Hiring Oversight Unit.

From these activities, OIG issues reports of findings and disciplinary and other recommendations to assure that City officials, employees, and vendors are held accountable for violations of laws and policies; to improve the efficiency, cost-effectiveness government operations and further to prevent, detect, identify, expose and eliminate waste, inefficiency, misconduct, fraud, corruption, and abuse of public authority and resources.

AUTHORITY

OIG's authority to produce reports of its findings and recommendations is established in the City of Chicago Municipal Code §§ 2-56-030(d), -035(c), -110, -230, and 240.

Cover image courtesy of OIG.

PUBLIC INQUIRIES:

NATALIE A. KURIATA: (773) 478-8417

NKURIATA@IGCHICAGO.ORG

TO SUGGEST WAYS TO IMPROVE CITY GOVERNMENT,
VISIT OUR WEBSITE:

[IGCHICAGO.ORG/CONTACT-US/HELP-IMPROVE-CITY-GOVERNMENT](https://igchicago.org/contact-us/help-improve-city-government)

TO REPORT FRAUD, WASTE, AND ABUSE IN CITY PROGRAMS:

CALL OIG'S TOLL-FREE HOTLINE

(866) 448-4754 / TTY: (773) 478-2066

OR VISIT OUR WEBSITE:

[IGCHICAGO.ORG/CONTACT-US/REPORT-FRAUD-WASTE-ABUSE/](https://igchicago.org/contact-us/report-fraud-waste-abuse/)