Citywide Privacy Protection Committee
2020 Final Recommendations

I. General Agency Policies and Guidance

General Agency Policies and Guidance Recommendation #1:

Guidance Supporting Internal Assessments of Identifying Information Law Compliance

It is recommended that the Chief Privacy Officer develop model protocols and policies that will provide guidance to Agency Privacy Officers with internal assessments for Identifying Information Law compliance.

Background: The CPO has provided APOs with a model agency compliance plan in the Agency Privacy Officer Toolkit. This compliance plan provides APOs with compliance tasks occurring at frequencies ranging from one time, with updates as necessary, to every two years. In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee observed that reporting often met minimum requirements without supporting context or information related to the specific steps taken to achieve compliance.

While the existing compliance plan remains an effective starting point, it could be enhanced with model protocols and policies that guide APOs in internally assessing Identifying Information Law compliance. For example, such a protocol might include guidance related to conducting periodic meetings with information technology and security personnel to discuss incident response. The developed guidance could be integrated into the model agency compliance plan in the Agency Privacy Officer Toolkit or set forth in a stand-alone document following the Toolkit approach. Model protocols and policies of this nature will support Identifying Information Law compliance and allow for APOs to provide more standardized and comprehensive reporting.

General Agency Policies and Guidance Recommendation #2:

Guidance Related to Languages

It is recommended that the Chief Privacy Officer provide guidance related to agency collection, retention, and disclosure of languages spoken by clients, employees, and vendors.

Background: In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee observed inconsistent reporting among agencies on whether languages spoken by clients, employees, and vendors is a type of identifying information that is collected, retained, and disclosed. Agencies should be collecting and using this data to inform their language access strategies. Agencies should also know if any privacy concerns exist around language access and how to protect such information, all to allow stronger language access services for limited English proficient clients. CPO guidance in this area, including whether

breach notification letters should be translated, will assist Agency Privacy Officers advise strategies related to language for their agencies.

General Agency Policies and Guidance Recommendation #3:

Guidance to Agency Privacy Officers for Disclosing Identifying Information in Response to Requests by Oversight Entities

It is recommended that the Chief Privacy Officer provide guidance to Agency Privacy Officers related to the disclosure of identifying information in response to requests for information by oversight entities.

Background: In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee found that APOs may benefit from guidance from the CPO related to responding to requests for information by agency oversight entities, which the Committee understands is already in progress. The legal authority of oversight entities to obtain information from agencies may create tension with the Identifying Information Law and Citywide Privacy Protection Policies and Protocols, particularly where oversight entities are not bound by other legal regimes for the protection of privacy. That tension may be compounded by the occasionally high-profile nature of oversight investigations, which may result in the disclosure of identifying information in a manner inconsistent with the Identifying Information Law and the Citywide Privacy Protection Policies and Protocols.

II. Emergency Management/COVID-19 Guidance

Emergency Management/COVID-19 Guidance Recommendation #1:

Ensure Communication with Agency Privacy Officers on Issues Related to Administration of Health Screenings

It is recommended that the Chief Privacy Officer, in consultation with the Law Department and the Department of Citywide Administrative Services, ensure that all Agency Privacy Officers are consulted prior to the rollouts of Agency-administered health screenings.

Background: The inclusion of APOs in the process will ensure that all APOs retain the opportunity to review rollouts of Agency-administered health screenings and provide feedback with respect to their own agency policies prior to the administration of health screenings. Any privacy-related issues related to the collection, access, retention, and disclosure of data in connection with health screenings should be addressed by APOs. To the extent that such policies have already been rolled out, APOs should be included in any further citywide discussions involving updating or expanding such policies.

Emergency Management/COVID-19 Guidance Recommendation #2:

Ensure Communication with the Agency Privacy Officers on Issues Related to COVID-19 and Other Public Health Emergencies

It is recommended that the Chief Privacy Officer, in consultation with the Law Department and the Department of Citywide Administrative Services, periodically hold conference calls with Agency Privacy Officer to provide updates and guidance related to the COVID-19 pandemic. In light of the current environment post-pandemic, in these meetings APOs will receive guidance on a variety issues such as the need to update remote work policies and agency agreements to account for remote work conducted by contractors, the need for model language for agreements, and guidance on contact tracing app usage.

Background: Given New York City's experience combatting the COVID-19 pandemic, which at times has required a dynamic response by agencies, establishing a forum and cadence for the CPO to provide COVID-19-related updates and guidance to APOs, as well as making those materials available in a centralized location, will support consistency and response efforts among agencies while remaining mindful of relevant privacy laws and policies. Additionally, recognizing that every emergency is unique, this approach can serve as a model providing guidance to APOs during future emergencies.

III. Agency Reporting Modifications

Agency Reporting Modifications Recommendation #1:

Changes to Reporting Format

It is recommended that the agency reporting template be updated such that information collected by the form can be transmitted into a centralized database.

Background: It is recommended that the agency reporting template be upgraded to a modern standardized fillable PDF form. Information collected can be transmitted into a centralized database.

Agency Reporting Modifications Recommendation #2:

Provide Additional Specificity and Content

It is recommended that the Chief Privacy Officer provide additional guidance regarding content and specificity of information captured in Agency Reports.

Background: Guidance from the CPO will ensure that information is entered as specifically as possible while remaining comprehensive. For example, broad terms such as "municipal agencies" should not be used unless they include details about level of specificity- e.g., naming parties or vendors to which agencies are disclosing identifying information.

Agency Reporting Modifications Recommendation #3:

Ensuring Historical Data is Collected

It is recommended that the Chief Privacy Officer require Agency Privacy Officers to document in each reporting cycle changes that were made from prior reports.

Background: This type of guidance will ensure that only sufficient responses are documented. For example, APOs will not be permitted to answer questions by stating "same as previous report" or "same as 2020." Such responses will be considered incomplete. Under the newly adopted modified reporting template, APOs will be required to indicate whether anything has changed from the previous report and if so, specify what changed from the previous report.

Agency Reporting Modifications Recommendation #4:

Clarification of "Routine" Designations

It is recommended that the reporting template be modified to reflect that in some instances, routine designations involving the disclosure of identifying information may also require additional legal review prior to disclosure. The Agency Report template should be clarified by including an asterisk next to the "routine" designation box, to reference the Agency Privacy Officer Toolkit, stating: "[i]n cases where the APO has designated an agency function as 'routine' and where identifying information is being disclosed to a third party, agencies should have an internal protocol in place to ensure that disclosures under such function have the appropriate level of agency legal review before the disclosure is made."

It is also recommended that the Chief Privacy Officer provide information regarding the legislative intent for the routine designation category. It is also recommended that the CPO issue further guidance regarding the interpretation of routine designations which would further clarify for Agency Privacy Officers how to distinguish between routine designations, and any further individualized review of items that fall under such routine designations, and case-by-case designations.

Background: The Identifying Information Law allows APOs to designate as "routine" certain collections or disclosures of identifying information. Collections and disclosures that are "routine" do not need further APO approval. In some instances, however, even when a routine designation has been made, the agency will need to have internal protocols designed to ensure that disclosure of information has the appropriate level of factual and legal review before the disclosure is made. In other words, just because a type of *function* is designated by an APO as "routine" does not mean that agency personnel can disclose any identifying information without further legal consultation. For example, an APO may designate as "routine" the function of responding to subpoenas, but the information ultimately disclosed in response to each individual subpoena will require legal review and authorization, based on the facts and laws that apply to the subpoenaed data.

It should also be noted that although not all "routine" disclosures will require this level of individualized review, certain disclosures may still require individualized review to ensure that the disclosure is legally permissible.

Agency Reporting Modifications Recommendation #5:

Monitoring the Impact of the Identifying Information Law

It is recommended that the Chief Privacy Officer use current agency reporting structures to assess how agencies are faring since the Identifying Information Law was enacted in 2018. The CPO should survey agencies to identify issues, challenges, and areas that need improvement.

It is recommended that the CPO hold periodic meetings to discuss how to address agency challenges and to discuss trending issues related to the collection and disclosure of identifying information that impact all agencies. It is also recommended that the CPO issue periodic reports to Agency Privacy Officers based on these findings.

Background: The CPO requires agencies to submit reports on a quarterly and biennial basis in compliance with the Identifying Information Law. Opportunity exists to use the information currently contained in the reports or to modify the reports to allow the CPO to analyze and monitor the impact of the Identifying Information Law on how agencies are protecting identifying information.

Agency Reporting Modifications Recommendation #6:

Improve Reporting for Community Boards and Engage Further with Community Boards to Determine What is Needed to Ensure Consistent Agency Report Completion

It is recommended that the Chief Privacy Officer survey community boards to determine how to make appropriate adjustments to the reporting process to ensure consistent report completion and assist community boards in their efforts to improve data protection procedures.

Background: It was recommended in 2018 that a different or simplified reporting template be developed for community boards that was better tailored to their limited functions. It was also suggested that the CPO consider issuing guidance that would assist community boards in completing the 2020 agency reports based on observations made during the 2018 reporting period. The CPO did provide the community boards with additional guidance in completing the agency reports for the 2020 period. However, review of the agency reports has indicated while it is believed that the community boards have the same or similar functions, there continues to be a lack of consistency with their reports.

Agency Reporting Modifications Recommendation #7:

Model Identifying Information Law Compliance Workflow and Guidance for Community Boards

It is recommended that the Chief Privacy Officer, in coordination with the Mayor's Community Affairs Unit and the Borough Presidents' Offices, develop a model Identifying Information Law

compliance workflow for community boards, including the preparation and submission of required reporting, as well as provide community boards with guidance on the implementation of the Citywide Privacy Protection Policies and Protocols and assistance with translating existing identifying information community board practices into policies.

Background: In reviewing the biennial Agency Reports, it was observed that community boards may benefit from additional guidance from the Chief Privacy Officer, including a model workflow for Identifying Information Law compliance, assistance with the implementation of the Citywide Privacy Protection Policies and Protocols, and assistance with translating existing identifying information practices into formal policy. There were varying degrees of identifying information collected and disclosed by community boards, including community boards in the same borough. Community boards often reported adherence to the Citywide Privacy Protection Policies and Protocols without providing supporting information on implementation. Community Boards also reported practices related to the handling of identifying information without connecting those practices to policies.

IV. Privacy, Technology, & Cybersecurity Coordination

Privacy, Technology, & Cybersecurity Coordination Recommendation #1:

Support of Collaboration Between Agency Privacy Officers and Chief Information Security Officers

It is recommended that the Chief Privacy Officer and the Chief Information Security Officer of the City of New York confer and discuss opportunities and means to facilitate collaboration and communication between APOs and agency CISOs.

Background: Recognizing the separate mandates and responsibilities of the CPO and the NYC CISO, there are considerable synergies and interactions between the disciplines of privacy and security. A cybersecurity program, through technical procedures (e.g., encryption) and policies (e.g., password management) maintains the confidentiality, integrity, and availability of systems and information, efforts which assist in the application of privacy principles. While the CPO and the Citywide Privacy Protection Policies and Protocols are mentioned at times in the Citywide Information Technology and Cybersecurity Policies and Standards, those policies were not regularly referenced in biennial Agency Reports. There are opportunities for further and more substantive collaboration regarding privacy and information security policies, which may support future utilization by APOs.

Additionally, while there are existing monthly meetings between the CPO and CISO, the substance of those discussions is not shared with APOs, who also do not currently have a mechanism for raising issues for consideration during those meetings. All APOs should be allowed to raise issues at this forum through the CPO.

Privacy, Technology, & Cybersecurity Coordination Recommendation #2:

Distribution of Cyber Guidance

It is recommended that the Chief Privacy Officer provide Agency Privacy Officers with any relevant updates provided by the New York City Cyber Command.

Background: In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee observed that, with agencies transitioning to remote work due to the COVID-19 pandemic, a majority of agencies did not mention COVID-19 or its impact on identifying information collection and disclosure, including agency policies related to working from home in their Reports. While New York City Cyber Command previously issued guidance in April 2020 to all Agency Chief Information Security Officers and Agency Chief Information Officers, the Committee identified that this guidance may not have reached all APOs.

Periodic updates of the policies and guidance which Cyber Command may provide to the CPO will mitigate the risk of future communication challenges. Further, with the increase in cyberattacks, cyber-related threats, ransomware attacks, phishing scams, and other opportunities for data security incidents, this distribution of knowledge will support APOs in advising their agencies regarding various information security issues that they should be informed about, and drive greater coordination and relationships between agency information security and privacy personnel.

Privacy, Technology, & Cybersecurity Coordination Recommendation #3:

Distribution of Standardized Sample Language

It is recommended that the Chief Privacy Officer promote awareness of City resources that assist Agency Privacy Officers with drafting and negotiating data sharing agreements, data security agreements, and other documents intended to secure agency data and systems.

Background: In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee observed that the documents that APOs often utilize, including data sharing agreements and data security agreements, may be enhanced by access to additional guidance and resources that exist around these documents.

The Committee understands that updates to templates for these documents are already in progress. When negotiating data sharing and data security agreements, agencies observed that vendors are often resistant to using City language and often insist that agencies use their language. While there are existing resources available to APOs, a knowledge gap regarding the existence of those resources was observed. Updates being distributed by the CPO, as well as making the existing resources available on the Mayor's Office of Information Privacy's Cityshare page, will address that knowledge gap, as well as allow for APOs to effectively engage with third parties during negotiations to ensure the interests of the City and its residents are sufficiently protected.

Privacy, Technology, & Cybersecurity Coordination Recommendation #4:

Guidance Related to Administrative Databases

It is recommended that the Chief Privacy Officer provide guidance related to the use of identifying information in administrative databases.

Background: In conducting its review of biennial Agency Reports, the Citywide Privacy Protection Committee routinely observed references to administrative databases without supporting information related to the governance of such databases, particularly with respect to identifying information. For example, several databases such as FMS, NYCAPS, and CityTime, among others, have users across all agencies with varying levels of access to data. Many of these databases do not have transparent rules for which users are allowed to access identifying information. Additionally, for new administrative databases under consideration, to what extent, if at all, is the need for identifying information considered? For existing databases, to what extent is there an evaluation of whether there is an ongoing need for identifying information collection and retention?