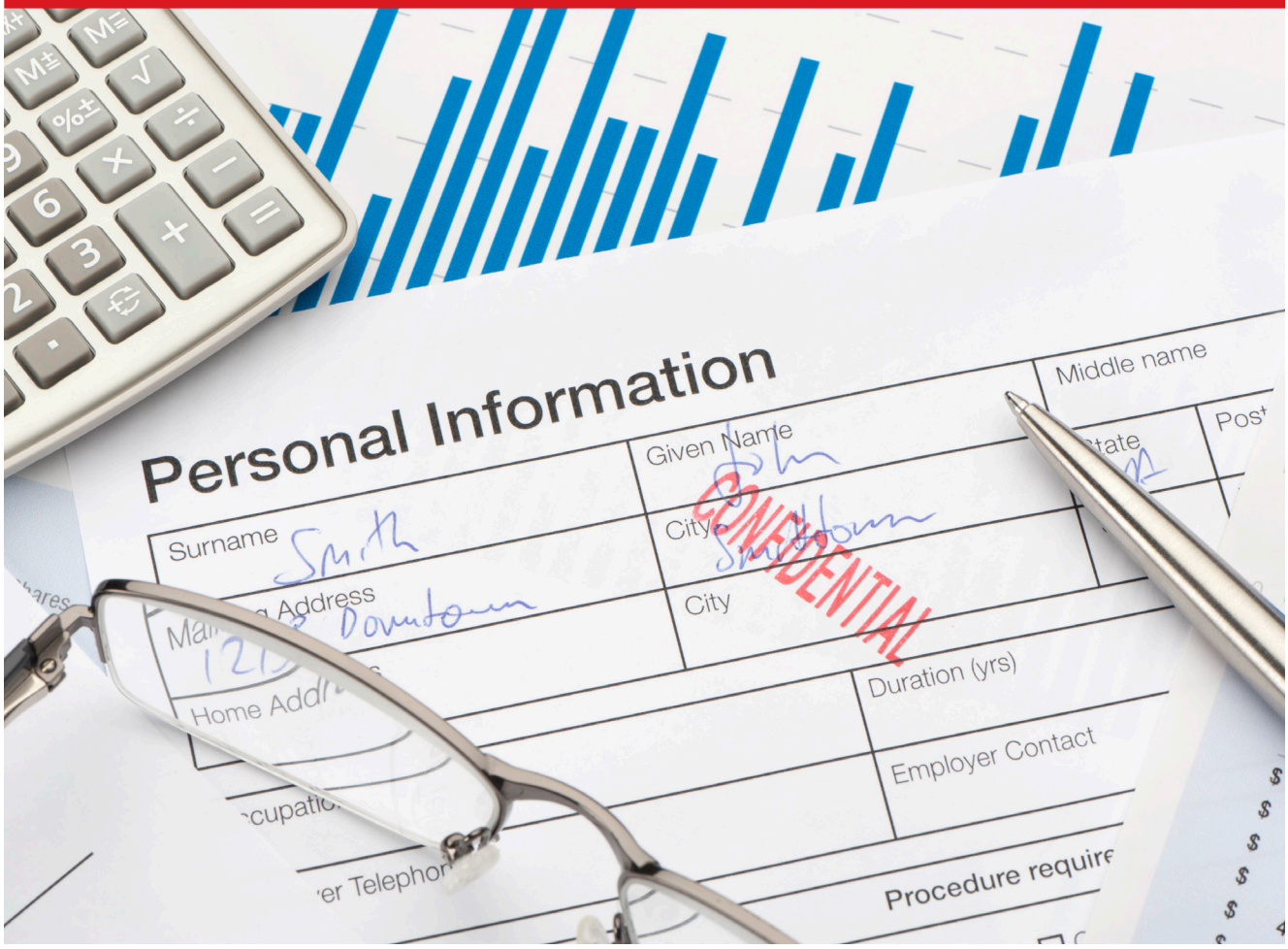
Some Progress Made But More Improvement Needed In Management of Personally Identifiable Information

July 1, 2019

A report by the Office of the District of Columbia Auditor



Audit Team
Joshua Stearns, Agency Risk Manager

Office of the District of Columbia Auditor

Kathleen Patterson, District of Columbia Auditor
www.dcauditor.org

Executive Summary

Office of the District of Columbia Auditor

What ODCA Found

Our work involved returning to the four agencies we audited in our 2017 report entitled "The DC Government Must Improve Policies and Procedures for the Protection of Personally Identifiable Information" to determine how conditions had changed. We found that progress has been made to identify and manage personally identifiable information at each of these four agencies. We also found that:

- The District Data Policy has provided a strong framework for agencies to gather and report information about which databases they have and which contain PII. In addition, it called for the secure storage and use of all sensitive data. OCTO, however, was unable to say with certainty to what extent PII data maintained by District agencies is being encrypted.
- OCTO hired a Privacy Counsel in 2017 to identify and develop policies that address privacy and PII. At the time of our interviews, the Privacy Counsel was in the process of working with other District agencies to develop this policy, which was anticipated to be made mandatory for all agencies subject to the authority of the Mayor.
- In interviews with senior OCTO officials, we learned of their efforts, together with the Executive Office of the Mayor, to pursue legislation that would clarify and strengthen OCTO's role to oversee and manage cybersecurity within the District of Columbia government.
- In 2018, DCHR and OCTO introduced an online course on cybersecurity that was made mandatory for all District of Columbia government employees. Most agencies reported very high compliance rates among their employees. OCTO officials said they hope to work with DCHR to introduce a new mandatory course in FY19 specifically about protecting PII.
- None of the agencies we revisited were yet implementing some of the PII management best practices according to the National Institute of Standards and Technology. These standards call for formal procedures to identify and manage PII within an organization, including conducting Privacy Threshold Analyses and Privacy Impact Assessments. OCTO has not helped agencies to perform these procedures.

Why ODCA Did This Audit

Cyberattacks and other breaches of sensitive personal data held by banks and other institutions continue to make the news and cause anxiety and worse for millions of Americans. The need for agency management and oversight bodies to monitor the risk of cyber-attacks within the District government is great. We determined that a follow-up engagement was important to keep the issue in front of the public and the District of Columbia Council. Accordingly, we reached out to the four agencies audited in 2017 to obtain an update on each of the findings from our earlier report.

What ODCA Recommends

While we did not develop new audit recommendations, we encourage management at OCTO and the other agencies to continue to strengthen their policies and procedures to mitigate the risks associated with collecting, managing, and using PII within their operations.

Table of Contents

Background

In January 2017, The Office of the D.C. Auditor (ODCA) published the results of an audit of the management and protection of personally identifiable information (PII) at four District agencies: the Office of the Chief Technology Officer (OCTO), the Department of Employment Services (DOES), the Department of Human Resources (DCHR), and the Child and Family Services Administration (CFSA). The audit, titled The D.C. Government Must Improve Policies and Practices for the Protection of Personally Identifiable Information, followed our audit at the Department of Youth Rehabilitation Services (DYRS), where we became aware of the potential for the wrongful use of PII. In addition, reports from the District of Columbia Office of the Inspector General (OIG) and the District of Columbia Homeland Security Commission (HSC) have, in recent years, highlighted the risk to information management assets, including datasets containing the personal information of District residents, taxpayers, and those receiving services from the District government.

All of this comes at a time when data breaches continue to make headlines around the country. In June 2015, the United States Office of Personnel Management discovered that the background investigation records of current, former, and prospective federal employees and contractors had been stolen. Stolen records included Social Security Numbers, usernames, passwords, and even fingerprints of millions of people. In October 2018, the United States Department of the Treasury's Office of the Inspector General reported that its audit had shown IT security weaknesses in several of the agency's national security systems.

Locally, on January 5, 2016, a former District government employee pled guilty to a range of charges stemming from their involvement in an identity theft and tax fraud scheme. Other noteworthy examples of the theft of personal information include the 2017 Equifax data breach, which exposed the sensitive personal information of more than 140 million Americans; the 2013 Target cyberattack that affected more than 41 million customers; and the 2014 breach at JPMorgan Chase, one of the nation's largest banks, that affected the sensitive personal information of 76 million households. Earlier this year, Wendy's agreed to pay $50 million to settle data breach claims from cyberattacks suffered in 2015 and 2016.

According to The U.S. Department of Commerce National Institute of Standards and Technology April 2010 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), when a person's personal information is stolen, they can suffer social, economic, or even physical harm. If the information stolen is sufficient to be used by identity thieves, victims can suffer a loss of money, harm to their credit, threats, and/or harassment. Losses don't end there, as individuals affected also can be forced to spend large amounts of time and money to address and recover from the damage. Other types of harm that may occur include denial of government benefits, blackmail, and discrimination. From the perspective of the District government, when there is a data breach, staff must spend time responding and agencies also may face a loss of public confidence.

It is with this background that we launched a follow up engagement in July 2018. The intent of this work was to review the conditions we found in our January 2017 report and determine whether the steps taken by the District government to address these conditions have led to improvements in the management of PII. In our previous report, we reported ten findings and issued eleven recommendations to the Mayor and various District government agencies. The findings and recommendations from that report are listed in Appendix A.

We have made inquiries to follow up on the implementation status of those recommendations but, given the importance of this issue and the pervasiveness of the risks involved, we felt it important to not just follow up on the recommendations but also to investigate the findings and conditions we discovered in our January 2017 report and report on what, if anything, has changed. This work did not involve a new audit and this work was drafted, reviewed, and approved in accordance with the standards outlined in ODCA's Policy and Procedure Manual.

In the conduct of this engagement, we reviewed legislation, regulations, and District agency policies and procedures related to the protection of PII. We also conducted site visits and interviews at selected agencies with management and employees involved in managing the collection and maintenance of PII. We used these interviews and limited document reviews to reach our conclusions about the status of PII management at OCTO, DOES, DCHR, and CFSA. This report is presented as a summary of what we found, noting what steps have been taken and how those steps have changed the PII management landscape in the District government.

District-Wide Actions Taken Since January 2017

D.C. Data Policy

On April 27, 2017, D.C. Mayor Muriel Bowser issued Mayor's Order 2017-115, the "District of Columbia Data Policy" (Data Policy). The Data Policy, which is applicable to all District agencies subject to the authority of the Mayor, called for the creation and maintenance of an inventory of all datasets held by District agencies, that each of these datasets be classified by level of sensitivity, and that this inventory regularly be made public. As of March 2018, OCTO had compiled an inventory of 1,640 datasets. These datasets covered a wide variety of contents and purposes, including those related to health, transportation, education, and public safety, to name just a few. While stating that the "greatest value" of the District's data "can only be realized" when the data is shared with other agencies, governments, and the public, the Data Policy also mandated careful management of this data to prevent identity theft and to protect the privacy and security of all those whose data was part of District government datasets. To this end, the Data Policy required that datasets requiring protection be identified and:

1. Regularly reviewed to determine whether the dataset is relevant and necessary to meet the current business needs and mission of the public body collecting the data.
2. Securely stored, transported, and otherwise technically and physically protected against unauthorized access, destruction, modification, disclosure, or loss.
3. Disseminated only to those persons and entities who reasonably require the information to perform their duties.
4. Reviewed to determine if useful derivative datasets can be created and publicly distributed by segregating sensitive portions of an enterprise dataset.[1]
5. Reviewed to determine if metadata[2] of derivative datasets or the combination of redacted datasets could result in the ability to accurately identify a person, and, therefore, jeopardize their privacy.

---

1 From the Data Policy: "Enterprise Dataset refers to a dataset that directly supports the mission of one or more public bodies. Typically, an enterprise dataset is stored in a named information technology system. For example, the District's general ledger is a dataset hosted in the System of Accounts and Records. Typically, such named systems and the datasets they contain are accessible to multiple workforce members. Any named system may hold one or more enterprise datasets."

2 From the Data Policy: "Metadata means a description of an enterprise dataset, such as date of creation or last update; author, maintainer, or point of contact; a dictionary to support the correct interpretation of data; and documentation of methodology or business rules."

6. Appropriately disposed of or archived when no longer needed.[3]

The Data Policy also established minimum data protection standards for all five classification levels established by the policy. Briefly, those five levels are:

- Level 0, Open
- Level 1, Public Not Proactively Released
- Level 2, For District Government Use
- Level 3, Confidential
- Level 4, Restricted Confidential

OCTO Hires Privacy Counsel

In 2017, OCTO hired a Privacy Counsel, to identify and develop policies that address privacy and PII. The incumbent has been working with representatives from other agencies to develop a set of policies and procedures to address basic minimum standards on how to manage PII in the District government. These standards are to be issued by OCTO and will apply to all District agencies under the authority of the Mayor but will not encroach on the ability of those agencies to create their own policies that go beyond the minimum standard. OCTO has not said when these policies will be finalized.

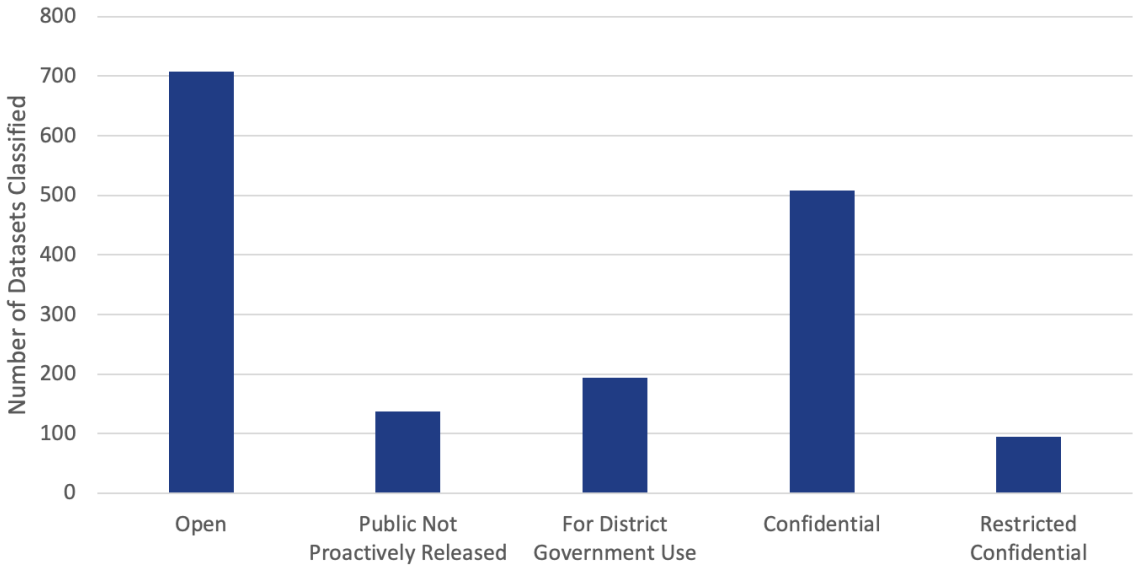
Enterprise Dataset Inventory

Pursuant to the Data Policy discussed above, OCTO led the development of an "Enterprise Dataset Inventory" in 2017. The Data Policy requires Mayoral agencies to record in the inventory all their datasets that directly support their missions. The Data Policy also requested that independent agencies participate in the development of the inventory. The Data Policy calls for annual reporting from the Chief Data Officer on the status of the Enterprise Dataset Inventory and efforts to address the twin goals of sharing and protecting the District's data.

In March 2018, OCTO published the first Annual Chief Data Officer Report (Report), which provided information about the status of efforts to develop the inventory. To that date, according to the report, 79 agencies had recorded 1,640 enterprise datasets. OCTO's report includes Figure 1, which shows how agencies classified the datasets included in the inventory.

3 Mayor's Order 2017-115. Paragraphs I(E) (1-5)

Figure 1: Classification of District Datasets



Source: Annual Chief Data Officer Report, March 11, 2018

Datasets containing PII typically were classified as Level Three, Confidential, the second most common.

OCTO also created a website that allows for the viewing and downloading of many of the enterprise datasets designated as open. The website includes many other features, including tools for building and development of apps that make use of the data. Information also is available that explains what many of the datasets show and why it is important or useful.

OCTO's Authority

Previous Findings

As part of work done for our January 2017 report, we concluded that the District lacked a central governmental IT authority.[4] We noted that the HSC 2013 Annual Report had found that the District lacked a senior executive-level Chief Information Security Officer (CISO) and that "there are no explicit CISO roles within any other District agency." Quoting further from the 2013 HSC report, we noted that it reported that "several agency officials expressed to the Commission that they were unsure of either their or OCTO's official roles and responsibilities in combating cyber incidents."[5] Based on our own work, we reported that OCTO was not monitoring the policies and procedures developed by District agencies and "does not know whether the agencies have in fact developed written policies and

4 This section updates Finding 1 from the ODCA January 2017 report, which states, "The District government lags behind the private sector in protection of PII because it lacks a central government IT authority." (p. 14).

5 The Commission's next annual report will update the 2013 one on cybersecurity.

procedures to protect PII." Finally, we reported that there was no central governmental authority responsible for: "determining whether all relevant District agencies are adequately protecting PII."

Existing Law and the Data Policy

The Office of the Chief Technology Officer was created by the passage of the Office of the Chief Technology Officer Establishment Act of 1998 (the Act).[6] The Act states that the purpose of the Office is: "to centralize responsibility for the District government's investments in information technology and telecommunications systems to help District departments and agencies provide services more efficiently and effectively. The Office will develop and enforce policy directives and standards regarding information technology and telecommunications systems throughout the District government."[7] Furthermore, the Act assigns a number of functions to OCTO, including: issuing regulations governing the "acquisition, use, and management of information technology…and resources…including hardware, software…"; and coordinating "the development of information management plans, standards, systems, and procedures throughout the District government…"[8]

The District of Columbia Data Policy sets forth a "comprehensive data policy for the District government"[9] applicable to all District government agencies subject to the administrative authority of the Mayor and gives OCTO primary authority and responsibility for carrying it out.

Furthermore, the Data Policy calls for the creation of two new positions: a Chief Information Security Officer (CISO) and a Chief Data Officer, each of whom are to "[further] implementation of and compliance with this policy." The policy also calls for the designation of Agency Information Security Officers and Agency Data Officers at each agency to assist with implementation of the policy "in coordination with … OCTO." The primary activity called for by the Policy, the creation of an Enterprise Dataset Inventory is to be managed by OCTO, which is instructed to create the data inventory as well as a "tool" to allow District agencies to contribute to it. OCTO is responsible for updating the inventory annually.

Agency Comments on OCTO's Authority

As part of our work on this report, we interviewed officials from DOES, DCHR, and CFSA. All three agencies acknowledge that OCTO is the central/guiding authority. Further, DOES and DCHR officials said that they complied with OCTO directives. CFSA explained that they depend on OCTO for "security and networking back end."

Proposed Legislation

The (then) interim Chief Technology Officer noted that OCTO's authority was dated and did not mention cybersecurity or PII because these were not issues of concern when OCTO was created. We were told by several senior officials at OCTO that they are working with the Mayor's office to develop legislation that would provide the

6 The Office of the Chief Technology Officer Establishment Act of 1998 is a subtitle within the Fiscal Year 1999 Budget Support Act of 1998, DC Law 12-175, effective March 26, 1999.
7 D.C. Code § 1-1402.
8 D.C. Code § 1-1403.
9 Mayor's Order 2017-115. Paragraph 1 (A).

additional clarity and authority over matters related to the protection of PII. Neither OCTO nor EOM have offered a timeline as to when this legislation will be introduced.

Actions Not Taken by OCTO

Despite having been given authority to oversee the way District agencies handle their PII, OCTO has not acted in several important areas. For example, OCTO can review District agencies' policies related to cybersecurity in general and PII in particular. According to officials inside OCTO, though, the agency has not reviewed any of the PII policies developed by District government bodies. Nor has OCTO yet developed a final District-wide PII policy for use by these bodies. (One is in development, see below.) OCTO has not helped agencies conduct either Privacy Threshold Analyses or Privacy Impact Assessments, as discussed in more detail below. Nor can OCTO say with certainty to what extent PII data maintained by District agencies is being encrypted per requirements contained in the Data Policy. We learned that OCTO is not working with agencies to ensure that the agencies' incident response plans (to address an incident of data loss or theft) are consistent with guidance issued by OCTO in 2016.

PII/Cybersecurity Policies/Procedures & Training

Mandatory District-Wide OCTO Cybersecurity Training and Planned PII Training

In 2018, DCHR introduced an online OCTO training course on cybersecurity that is mandatory for all District government employees. The course included material on how to defend against cyberattacks of all kinds and best practices on how to keep government information safe. As of late in 2018[10], most District agencies had very high completion rates for their employees. Among the employees in Mayoral agencies, the completion rate was 76%. Some bigger Mayoral agencies, though, had lower completion rates. For example, DCPS had only a 48% completion rate, and DPW had only a 68% completion rate. Among the agencies that we examined as part of this engagement, the rates were: OCTO – 96%, DCHR – 100%, CFSA – 97%, and DOES – 98%.

In addition, OCTO officials explained that it is their intention to introduce a new mandatory course specifically about PII protection for all District government employees in 2019. This course also will be available online to employees.

Planned District-Wide PII Policy

As mentioned previously, OCTO is working on a District-wide PII policy.[11] The policy would apply to all District agencies and would set minimum standards for managing and protecting PII gathered by the District government. This policy is being developed by a team within OCTO led by the Privacy Counsel. There are also representatives on the team from other agencies. OCTO would not share a draft, indicating that it was not complete, but multiple officials said it would be coming soon. Then Acting Chief Technology Officer Barney Krucoff mentioned the agency's plans to release such a policy at the November 2018 meeting of the Open Government Advisory Group, a group

10 We received an undated report from DCHR with this information on October 31, 2018.
11 This section updates Finding 2 from the ODCA January 2017 report, which states: "The District does not have government-wide policies and procedures for documenting the identification of PII it collects." (p. 16).

whose members are tasked with evaluating the District government's progress in improving transparency, openness in government, and sharing more of the data gathered by the government.

What We Found at the Agencies

While conducting this follow-up engagement, we visited DOES, DCHR, and CFSA to ask about their PII policies and what training they provide to staff on proper PII management.[12] Officials from all three agencies were very forthcoming and open in their responses to our inquiries. We summarize what we found below.

DOES

DOES has two policies, Handling Sensitive Information and Data Integrity, that collectively cover different aspects of proper PII management and safeguarding. One of these policies was in existence when we published our January 2017 report and one has been updated since that time. Neither, however, address collecting PII data.[13] According to DOES officials, all staff have been notified of the existence of these policies and are provided with training on proper PII management. However, the training demonstrated was an online tutorial that staff were expected to take by themselves. After reviewing this tutorial, it was not clear that it related directly to DOES's own policies and procedures. Instead, it appeared to cover PII management from a generic perspective. Further, DOES did not provide documentation demonstrating that these trainings have taken place.

DCHR

DCHR shared with us a PII policy that was updated in October 2018. In interviews, DCHR officials also said it has eliminated unneeded PII questions when developing new forms. This process of eliminating unneeded PII collection when creating new forms, however, is not written down and so appears to be informal. Their written policy does not address data collection.

DCHR explained that the 2018 PII policy update was in the process of being distributed at the time of our follow-up. According to an Associate Director at DCHR, staff will be required to sign a form acknowledging receipt. DCHR was able to share with us certain documentation showing training materials related to PII, but they did not provide documentation of who at DCHR has received the training and when.

CFSA

CFSA finalized a PII policy in August 2018 with language that addresses the collection of PII, including:

---

12 This section updates Findings 3, 6, and 7 from the ODCA January 2017 report. Finding 3 states: "CFSA, DCHR, and DOES do not have policies that govern data collection." (p. 18). Finding 6 states: "Sampled agencies have written PII confidentiality policies and procedures by they are not always comprehensive, consistent across agencies or distributed to relevant employees." (p. 20). Finding 7 states: "CFSA, DCHR, and DOES security training was neither consistent nor conducted on an annual basis.

13 Policies that address collecting PII data would include provisions requiring, for example, an analysis of whether certain PII is really needed to conduct the operation in question. Other examples might include provisions ensuring that PII is not collected twice from the same customer. DOES's policies do not include these kinds of provisions.

"CFSA shall:

- Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.
- Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.
- Conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings quarterly to ensure that only PII identified in the notice is collected, retained, and that the PII continues to be necessary to accomplish the legally authorized purpose."[14]

Our contacts at the agency explained in September 2018 that they would distribute the new policy via email to all employees. However, as of March 2019 CFSA said that this has not yet happened.

CFSA officials explained that new employees had been given the training on CFSA's previous PII policies as part of their on-boarding of new employees and provided us with documentation. In addition, employees whose work involves the Statewide Automated Child Welfare Information System, a software program that CFSA uses to administer certain federally-funded programs, are shown a training video whenever there are updates to this system. We were told that these updates happen as frequently as twice a year, so relevant employees are reminded of the importance of protecting PII regularly.

Other Agency and OCTO Actions

De-identification

In our January 2017 report, we concluded that CFSA, DCHR, and DOES were not "de-identifying" PII across all divisions within those agencies.[15] De-identification is a process by which PII is removed or obscured from a record or file so that there is no reasonable basis to believe that the remaining information can be used to identify an individual. De-identification is important when sharing data or records, such as when creating a summary report about agency performance.

In our interviews for this report, neither CFSA, DCHR, nor DOES could say with certainty that they were systematically de-identifying information as a matter of agency policy or practice. DCHR has changed the way one of their key forms, the SF-50, displays information when printed. The SF-50 is used to record many kinds of personnel actions, such as hiring, raises, promotions, etc. It has been modified so that it displays only the last four digits of a person's SSN when printed. However, the form still clearly has the person's name on it, so this change is not enough to consider the record to have been de-identified. The agency did make clear that they completely de-identify data when responding to FOIA or other requests from outside the agency.

14 Child and Family Services Agency. Personal [sic] Identifiable Information. Policy Approved August 31, 2018. (p. 4).
15 This section updates Finding 4 from the ODCA January 2017 report, which states: "CFSA, DCHR, and DOES do not de-identify PII across all divisions." (p. 18).

Privacy Threshold Analyses

According to NIST, "organizations are required to identify all PII residing within their organization or under the control of their organization through a third party." One way that organizations can conduct this important work is through a structured process called a Privacy Threshold Analysis (PTA). PTAs can be simple questionnaires that are completed by the owner of a database or system working together with the owner of the data located within the system. These questionnaires would identify whether PII is present, what privacy requirements apply to the system, and whether a Privacy Impact Assessment is required.

In our interviews with the then interim CTO and the then interim CISO, they explained that they have not provided assistance to District agencies in conducting PTAs or similar analyses. Neither DOES, DCHR, nor CFSA reported that they had conducted formal PTAs, although all were familiar with what they were and CFSA said they were planning to conduct such assessments in the future.

The District of Columbia Data Policy required all agencies to report on the existence of all of their "enterprise" databases and to classify the same. One of the classification levels, Level 3, includes data that is protected from disclosure under a variety of legal and regulatory requirements. For those agencies that have complied so far with the requirements of the Data Policy, an identification of which datasets contain PII would have had to have been completed, even if this process was not done pursuant to a PTA structure or policy. Consequently, the process of compiling and classifying datsets pursuant to the Data Policy resulted in agencies identifying which of their datasets contained PII, even without having a separate Privacy Threshold Analysis policy in place.

Privacy Impact Assessments

In the "Guide to Protecting the Confidentiality of Personally Identifiable Information," NIST describes Privacy Impact Assessments (PIAs) as "structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system." [16] While Privacy Threshold Assessments are essentially simple surveys to identify which databases contain PII, the PIA is the next step – where organizations can begin to identify what the relevant laws and regulations are that they must comply with, what the risks are from collecting and holding PII and evaluate processes for mitigating those risks. Our January 2017 report recommended that the Mayor require all agencies to conduct PIAs or a similar assessment to mitigate privacy risks.

Neither CFSA nor DCHR have done formal, documented PIAs. The current CFSA PII policy calls for them to be conducted but the agency had not yet done so at the time of our interviews.

OCTO officials said that they have not helped agencies conduct formal PIAs but sometimes do evaluations on a case-by-case basis with agencies when they are developing new systems. As mentioned above, the District Data Policy requires that agencies should:

"Regularly review [datasets containing PII] to determine whether the dataset is relevant and necessary for meeting the current business needs and mission of the public body collecting the data."

This requirement to review the need to collect PII is similar to the requirements of a PIA as defined by NIST although

16 This section updates Finding 5 from the ODCA January 2017 report, which states: "CFSA and DCHR do not conduct Privacy Impact Assessments." (p. 19).

it is not as clear about the need to identify and mitigate risks.

Encryption

Our January 2017 report included two findings related to encryption. [17] One noted that the subject agencies (DOES and DCHR) did not "require that all end-user[18] storage devices be encrypted." The second reported that "not all DCHR and DOES databases are encrypted." We returned to these two agencies to inquire again about the encryption of data containing PII.

DOES

DOES officials explained the difficulties they face in encrypting entire databases. To do so would result in unacceptable loss of efficiency in doing their day-to-day work as their systems would become too slow in attempting to access the encrypted data. Instead, they explained, they are looking at encrypting only those data tables or other elements that contain PII, which will reduce the data processing load. Because some of their data resides on servers controlled by OCTO, DOES officials were not sure whether they could accomplish full encryption without OCTO's help.

DOES's Data Integrity Policy requires end-user storage devices with PII to be encrypted. Officials from the agency further explained and demonstrated that those divisions within the agency where PII would often or usually need to be displayed on computer screens or otherwise used at employees' desks are in secure portions of their building. Entry into these offices is controlled and only authorized personnel may gain access. In an interview with DOES's Chief Information Security Officer and his staff, they were able to demonstrate the internal controls in place to ensure that all relevant laptops at DOES are equipped with full disk encryption. In addition, DOES desktops do not accept thumb drives, a further security measure to ensure that data is not stolen or inadvertently misused.

DCHR

When asked whether their databases containing PII are encrypted, DCHR explained that because their servers are owned and maintained by OCTO, they cannot act on their own to encrypt them. Nevertheless, they also let us know that the servers containing PeopleSoft, the primary software/ database used to manage District employees' information, have been encrypted. When asked about progress in encrypting databases containing PII District-wide, the then-Interim Chief Technology Officer told us that DCHR was "largely done," and that PeopleSoft was encrypted. DCHR said that within their office, they use a Secure Print system that restricts the ability to print documents containing PII.

DCHR told us that their laptops are encrypted using Bit Locker and described the process used to ensure compliance with this policy. We asked for, and were provided, a list of DCHR laptops showing encryption. In

17 This section updates Findings 8 and 9 from the ODCA January 2017 report. Finding 8 states: "DCHR and DOES do not require that all end user storage devices be encrypted." (p. 22). Finding 9 states: "Not all DCHR, and DOES databases are encrypted." (p. 22).

18 "End-user storage devices" are typically portable devices capable of storing electronic data, e.g., laptops, thumb drives, etc.

a meeting with several DCHR employees, one was able to show an ODCA auditor that her laptop was, in fact, encrypted. It was not clear from this small sample whether all DCHR laptops were, in fact, encrypted. DCHR further said that they use Airwatch to encrypt emails to and from approved devices.

OCTO

In interviews, OCTO officials explained the technical challenges involved and progress made so far in encrypting District government databases containing PII. They said that all OCTO-managed databases are protected using SSL technology and that OCTO has been quite active in obtaining SSL certificates for the servers containing these databases.[19] At the same time they indicated that the agency manages and houses databases for which OCTO currently only has limited ability to enforce compliance with recommended encryption standards.

Some agencies have been more proactive in reaching out to OCTO and asking for help in encrypting their PII data. In general, OCTO has been handling the encryption of databases containing PII on a case-by-case basis. The then-Interim CTO explained to us that part of the complication in encrypting data is that both the back end (the server containing the data) and the front end (the software being used to access the data) need to be able to "talk" to each other and if OCTO takes steps to encrypt the servers, this can sometimes interfere with the communication between the two. In this case, because OCTO does not have control of the software used within each agency, acting to encrypt databases without coordination with the agencies can have negative consequences.

For this reason, the interim CTO's position was that the timing of encryption sometimes would have to be delayed until the agency had the funds and was otherwise prepared to upgrade their software and that it would not make sense to do the work required to encrypt the data and then have to do all the same work again soon after new software was installed. He acknowledged that there was currently a "dearth of master planning" that would be needed to allow this process to proceed in an efficient manner.

OCTO officials explained that encrypting laptops and other "end-user devices" involved a lot of local IT support, but that a lot of smaller agencies don't have the capacity. The interim CISO told us that they were rolling out Bitlocker to DC government-issued laptops but acknowledged that it was a "long-term" project to make encryption happen on all such devices.

Incident Response Plans

As part of NIST's Framework for Improving Critical Infrastructure Cybersecurity, the core functions for managing cybersecurity risk include: *Identify, Protect, Detect, Respond, and Recover.* [20] In April 2016, OCTO issued the "Cyber Security Incident Response Team Policy," applicable to all D.C. government agencies and establishing a common framework that agencies were to adopt when responding to cybersecurity incidents. All security incidents were to be referred to OCTO for handling and agency IT personnel were to participate in a Cyber Security Incident Response Team, coordinated by OCTO. However, none of the three agencies we spoke with mentioned this policy and two said

19 Secure Socket Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client.
20 This section updates Finding 10 from the ODCA January 2017 report, which states: "CFSA, DCHR, and OCTO have not developed an incident response plan." (p. 23).

they had no knowledge of its existence. Even OCTO officials could not say whether agencies were complying.

Our 2017 report focused on CFSA and DCHR with regard to their lack of incident response plans. When we returned to CFSA and asked about their incident response plan, we were given a flowchart showing how the agency would respond to cybersecurity incidents. It was not in compliance with OCTO's 2016 policy directive. Later they informed us that they were working on an update to their plan. A portion of DCHR's PII policy addresses incident response. It does not appear to be in compliance with OCTO's policy.

The District government has taken additional steps to mitigate the risks posed by cyberattacks. In 2018, The Office of Risk Management partnered with OCTO and the Homeland Security and Emergency Management Agency to purchase a cyber insurance policy. The policy pays out in the event of a cyberattack and, therefore, helps offset the costs associated with data breaches. In addition, it includes access to specialists who will be able to assist the District with its response, potentially minimizing the damage done during an ongoing attack and/or identifying weaknesses that can be fixed to reduce the chances of additional loss.

Conclusion

Our review of current conditions at OCTO, CFSA, DOES, and DCHR revealed improvements in the way the District government is managing its PII. The data collection efforts begun pursuant to the District Data Policy have increased the attention given to some of the basic components of proper PII management. For example, agencies are now more aware of what datasets they have, and which ones contain PII. In addition, OCTO has begun hosting routine meetings for Agency Data Officers and for Agency Information Security Officers where those officials can hear from their OCTO counterparts as well as share information among themselves on a variety of topics, including those relevant to ensuring that PII is gathered and maintained in a secure manner.

We learned from OCTO of plans to release a PII policy which will apply to all District agencies subject to the authority of the Mayor. According to OCTO officials, the agency has also been working with the Executive Office of the Mayor to craft legislation to further clarify OCTO's role in leading the District government's efforts to maintain cybersecurity. If and when the policy is announced, and the legislation is introduced, they promise to provide needed tools to help manage the risk posed by cyber threats.

On the other hand, there are still areas of concern. There does not appear to be a comprehensive incident response policy in place should one or more District agencies face a cyberattack such as those that continue to make news. It is troubling that, even after having issued a policy on incident response that was nominally mandatory for all District agencies, OCTO officials could not say whether any agencies were in compliance with it. None of the agency incident response plans we reviewed appeared to be and none of the agency officials we met with were aware of the OCTO policy. The purchase of cyber insurance is a positive development, but until there is more coordination, the risk remains.

PII management continues to appear somewhat informal at the agencies other than OCTO that we reviewed. While there is no reason to expect that policies and procedures would be identical from agency to agency, it is still worth noting how differently each agency treated the development, distribution, and training on those policies and procedures. In some cases, it appears there was no written procedure governing key processes.

Threats related to cybersecurity remain at the top of most lists of risks facing organizations around the world. The risk is not a static one, as cyber threats are constantly changing. The District of Columbia government would be wise to continue pressing forward with its efforts to manage cyber threats, investing in improved policies, tools, training, and knowledge. The consequences of a significant attack could be quite severe, not only for government operations, but also for the individuals whose personal information could be stolen and then used to their detriment.

Agency Comments

On May 6, 2019, we sent a draft copy of this report to the OCTO, CFSA, DOES, and DCHR. All four provided comments between May 17–24, 2019, which are included here in their entirety, followed by ODCA's response.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Child and Family Services Agency

May 20, 2019

Kathleen Patterson
District of Columbia Auditor
717 14th Street, NW, Suite 900
Washington, DC 20005

Dear Ms. Patterson:

Thank you for sending your team's updates on the recommendations from the District of Columbia Auditor's (ODCA) audit of personally identifiable information (PII) published in January 2017. My team has been working closely with yours to identify improvements to the Child and Family Services Administration (CFSA) policies and systems.

As a result of that cooperation, CFSA created an Incident Reporting policy (see attached). This policy is continuously being updated and improved based on industry practices and lessons learned from actual events.

In addition, attached to this letter is a document which includes CFSA's responses to the recommendations in Appendix A of the draft report and also the Plan of Action and Milestones (POA&M) for the outstanding recommendations in Appendix A of the draft report related to CFSA, specifically item numbers 4 through 6 and item 8.

Thank you for your thorough assessment. If you have any questions please contact Marina Havan, our CIO, at 202.434.0012.

Sincerely yours,

Brenda Donald
Director

Cc: Joshua Stearns, ODCA, Agency Risk Manager
Racheal Joseph, CFSA, Chief of Staff
Marina Havan, CFSA, CIO

POLICY TITLE: Information Technology Incident Response CHAPTER:		PAGE 1 OF 8
	CHILD AND FAMILY SERVICES AGENCY Approved by:_____ Signature of Agency Director	PROFESSIONAL STANDARDS See Section VII.
EFFECTIVE DATE:	LATEST REVISION: March 3, 2011	REVIEW BY LEGAL COUNSEL: March 17, 2011

I. AUTHORITY	Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, published at 45 C.F.R**.** Parts 160, 162, and 164 (Security Rules); 45 C.F.R. § 164.310 (a) (1), § 164.308 (a) (6), Security Incident Procedures. Facility Security Plan; DC Official Code § 2-213.01; DC Official Code § 2-213.02; DC Official Code §1-1135, b, (6); DC Law 5-168, 4, § 32 DCR 721; DC Law 11-259, § 305(a), 44 DCR 1423; DC Law 12-175. Act 12-239; "HITECH ACT" 42 U.S.C. § 17932
II. APPLICABILITY	Full or part-time Child and Family Services Agency (CFSA), also referred to as the Agency, employees; contractors who are authorized to use CFSA's equipment or facilities; and volunteers who are authorized to use and have been provided with a user account to access CFSA resources.
III. RATIONALE	This policy establishes guidelines for the CFSA to comply with the Information Security Incident Procedures Standard 164.308(a)(6) of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, ("HIPAA"). The purpose of this policy is to establish a process to report information security incidents, mitigate any harmful effects, and document the outcome of security incidents. In addition, this policy will reflect CFSA's compliance with industry best practices, and or, where applicable, District, and federal regulations.
IV. POLICY	The CFSA is legally obligated to protect private electronic information of children and families receiving services from the Agency. The CFSA workforce members shall report to the CFSA Office of Risk Management any suspected or known information security incident that may have a negative impact on CFSA's Information Technology (IT) resources, violates CFSA's information security policies and procedures, or circumvents information security mechanisms and requires immediate action to prevent further negative impact immediately. If applicable, the Office of Risk Management and the HIPAA Privacy Officer shall notify the CFSA Information Security Officer (ISO). The ISO shall notify the Office of the Chief Technology Officer (OCTO) Helpdesk as appropriate.

V. CONTENTS	**A.** Information Security Incident Reporting **B.** Information Security Incident Response Procedures **C.** Information Security Incident Reporting and Tracking **D.** Information Security Incident Triage **E.** Escalation **F.** Diagnosing an Information Security Incident **G.** Notifications and Actions **H.** Information Security Incident Resolution **I.** Document Findings **J.** Follow-up **K.** Roles and Responsibilities **L.** Responsibility for Maintenance and Compliance **M.** Disciplinary Action for Violations
VI. ATTACHMENTS	**A.** Definitions **B.** CFSA Information Technology Incident Report Form **C.** CFSA Property Release Form
VII. PROCEDURES	**Procedure A: Information Security Incident Reporting** 1. Using a set of predefined procedures provides insurance that an incident must be handled with a minimum of adverse impact on customers and the IT resources. In reporting a information security incident, the following actions are required: a. If a workforce member becomes aware of an information security incident issue such as a stolen or lost laptop, system virus or absence email, he or she should first report the problem to his or her supervisor, call the IT ServUS Help Desk at 202-671-1566, and then complete the Computer Incident Form. b. The designated CFSA Computer Security Incident Response Teams (CSIRT) will define the roles and responsibilities of CFSA staff during an incident and ensure that the standard procedures are being followed when responding to or communicating an incident. Using a set of predefined procedures, provides assurance that an incident shall be handled with a minimum of adverse impact on customers and the IT resources. 2. The CFSA CSIRT Team should comprise of the Chief Information Officer (CIO), Supervisory Information Technology Specialist (Network Services), Information Security Officer (ISO), Risk Management Specialist (RMS), HIPAA Privacy Officer and technical support personnel. Each will respond base on the expertise required to resolve the incident. 3. Without specific details in the report that can be verified, an incident may be considered insufficient. The CFSA CSIRT shall provide guidelines for CFSA staff to include helpdesk personnel; network system engineers Managers/Senior Staff; OCTO IT Security Team for responding to computer virus, malicious logic, and technology service interruptions. The guidelines must be applicable for networked systems and infrastructure that include:

a. A User workstations and common network equipment (facsimile, printers, etc.)

b. Host systems providing services to multiple users (file servers, timesharing systems, database servers, Internet servers, Email servers, etc.), LAN or WAN

c. Direct connections, gateways, or modem access to and from external networks, such as the Internet Telecommunications switches, data communications and telephone lines

4. The CFSA Chief Information Officer shall make available a designated response staff to provide incident response support via telephone, from 8:15 a.m. to 4:45 p.m., EST/EDT. During non-business hours, continuous support shall be provided via cell phone and a telephone voicemail system. Incidents reported on the voicemail during non--business hours are responded to within one (1) business day. "On call" response staffs must be equipped with cell phone, personal computers, and Internet connectivity to facilitate immediate response to incidents reported during non-business hours.

Procedure B: Information Security Incident Response Procedures

1. An information security incident response shall be required to protect and support CFSA IT resources from known incidents, notify information managers, and take steps to ensure that CFSA staff uniformly informed of security events and occurrences. The procedures described here must be performed when:

   a. Either an end user reports an incident to the Helpdesk

   b. IT technical support staff discovers an incident

   c. If a HIPAA incident has been reported to the Office of Risk Management

Procedure C: Information Reporting and Tracking

1. All CFSA computer network users and workforce members are directly responsible for:

   a. Reporting information security incidents immediately to their supervisor and the IT ServUS Help Desk

   b. The IT ServUS Help Desk must notify the Agency Information Security Officer (ISO)

   c. The ISO must notify the appropriate response team members to assist with resolution and notification of the incident. The incident shall be reported <u>within one (1) business day of the first occurrence</u> to OCTO.

2. The following information must be recorded in the IT ServUS help desk tracking system and/or the Computer Incident Report Form (Attachment B):

   a. Current date & time of incident reported

   b. Name, phone, email, and Agency affiliation of person reporting

incident

c. Type of incident (security exposure) when known

d. Affected system name and number of users impacted when known

e. Description of incident, include applicable Change Control Board (CCB) number when appropriate

f. Actual or estimated date and time the incident occurred

g. Actions taken and estimated time to implement resolution(s)

h. Name and support area for who resolved the Incident.

3. After the information is recorded, an investigation shall start immediately. CFSA's Security Officer shall produce an investigative report under the direction of the District Security Official (DSO). The report must be submitted to the DSO for approval. In special situations, the DSO may conduct the investigation for the covered Agency.

Procedure D: Information Security Incident Triage

1. A workforce member or a technical support staff who may first notice an incident must report it to the IT ServUS Helpdesk. Assigning an incident with a level of severity helps to ensure that the incident receives adequate response for a resolution. In order to manage reported events, each incident must be assigned to one of four categories as indicated below:

   a. Need to add Protected Health Information (PHI) incident to these tables (e.g., 1to 5 PHI accounts Severity 4 and so on); then determine the CSIRT team.

Severity 1	Incidents that involve an outage that is considered disruptive on a major scale (e.g., loss of connectivity to any mission critical systems and applications). This level of severity may be defined as an emergency and always requires executive review and authorization to implement corrective action.
Severity 2	Incidents considered moderately disruptive but capable of causing extreme delays or potential impact to multiple users (e.g., non-mission critical systems or resources). This moderate level of severity may require executive review and authorization to implement to corrective action.
Severity 3	Low-level incidents routinely addressed and isolated with minimal or no impact to users or production systems (e.g., password suspensions). This level of severity usually does not require executive review and authorization to implement corrective action.
Severity 4	Concern for follow-up activity but does not require immediate executive review and authorization to implement the corrective action:

Triage	Escalation	Event
1st Tier	IT Service	All Reported Incidents
2nd Tier	Incident Response Team	Emergency (severity 2,3)
3rd Tier	Senior Management	Emergency or Critical Failure (severity 1, 2, 3)

Procedure E: Escalation

1. To assist in centrally managing incident tracking and resolution, the IT ServUS Helpdesk will perform first tier incident determination on all incidents reported by users and will provide resolution whenever possible.
2. When second tier support is necessary, the IT ServUS Helpdesk will escalate the incident to the appropriate predetermined support area for action. At that time the IT ServUS Helpdesk shall notify a contact via e-mail, voice mail, cell phone or cell phone until contact is established and the incident is assigned. If the IT ServUS Helpdesk is unable to assign a contact within 20 minutes during regular business hours, the incident shall be escalated to the appropriate Manager (third tier).
3. The following steps are required:
   a. All minor incidents must always be resolved at the lowest possible level of escalation by the IT ServUS Helpdesk. In turn, the IT ServUS Helpdesk shall report the problem to the ISO or the appropriate Response Team Member.
   b. Following notification to the IT ServUS Helpdesk, severe incidents that have a high probability of causing extreme delays or impacting multiple users or areas shall be escalated to the Supervisory Information Technology Specialist (Network Services) and/or the CIO.
   c. The senior management with authority to take action outside of standard operating procedures shall be notified if the first and second levels of interactions are unsuccessful in resolving operational incidents

Procedure F: Diagnosing an Information Security Incident

1. The first steps in determine if the incident is a security issue or a system administration issue, the individual must identify, isolate, and analyze the incident. For example, when a user cannot remember his or her password, it is a system administration issue and the system administrator should be contacted. If a user opens a file through email and there is an immediate mass email distribution or system crash, then this could be a security incident. The following is a representative list of indicators that a security incident may be occurring:

Symptom	Potential Incident
System crashes unexpectedly	New user accounts are created which bypass standard procedures
Sudden high activity on an account that has had little or no activity for months	New files with unusual names appear
Accounting discrepancies	Unexplained or unauthorized
Changes in file lengths or modification dates	Attempts to write to system files
Data modification or deletion	Denial of service
Poor system performance	Suspicious probes
Suspicious browsing patterns	Virus attacks via email
Unauthorized port scan	Loss of mainframe connectivity
Disrupted Telecommunications service	Unauthorized data transmission

2. The Response Team member must perform the following minimum tasks during the diagnostic stage of incident resolution:
   a. Review current access or concern with appropriate individuals and management
   b. Identify appropriate solution
   c. Communicate intended changes with the affected users and include management for major changes to assess impact to business areas
   d. Establish testing to avoid interruptions when appropriate
   e. Trouble shoots potential problems
   f. Schedule an implementation plan with applicable back out

Procedure G: Notification of Actions

1. Ownership of an incident resolution must be assigned to the area responsible for maintaining the impacted service. Once reported incidents are categorized as severity levels 1 & 2, certain corrective actions may require senior management authorization as well as CCB oversight.
2. Based on the nature and scope of the incident, the Agency Supervisory Information Technology Specialist (Network Services) shall make the decision to clarify whether the incident can be resolved within the Agency, or whether additional help is required from OCTO or other outside services. However, if an intrusion is in progress, the Supervisory Information Technology Specialist (Network Services) or CIO shall make a risk-based management decision to leave the network connected for detailed analysis or disconnect.
3. The following actions are required for managing notifications and alerts:
   a. The initiator of the report shall reply by telephone (not cellular) within 15 minutes to an incident coordinator

	b. Information about the incident shall be collected from the reporting entity, including the caller's name, affiliation, location, and incident details c. The incident coordinator shall perform an immediate initial assessment to evaluate the category of the incident
	Procedure H: Information Security Incident Resolution 1. The incident shall be recorder via the IT ServUS Help Desk and assigned a tracking number. If CCB is applicable, a number must be assigned by the technical team. Upon submission of the final reports to the ISO, the IT ServUS Help Desk shall be advised to follow up with the incident caller and close the tracking number. 2. For unauthorized access, denial of service, misuse of IT resources, hostile probes, and other concerns, the Supervisory Information Specialist (Network Manger), along with his technical staff, shall resolve the issue, document incident details and follow up with the ISO during business hours by the next business day. 3. At the point that an appropriate solution is accepted and ready to implement, support staff must stand by to confirm the following status: a. Verify successful implementation with user(s) b. Trouble shoots subsequent problems c. Verify successful implementation d. Report task as completed 4. Additionally, when an incident can be resolved within the Agency, the coordinator must work with CFSA technical personnel to complete and shall document all task performed as needed, which include: a. Copy log files b. Review log files c. Check binaries and configuration files d. Rectify intruder modifications and clean or reinstall system e. Contact other/remote sites if necessary f. Restore the system to normal operations g. Update Helpdesk knowledgebase h. Update documentation procedures and contact lists i. Update configuration and backup files j. Review protocol and Service Level Agreements with vendors *Note: Depending on who reported the call and the nature of the call, no additional notification of resolution to any entity may be required.*

	Procedure J: Follow-up The individual assigned to resolve the incident shall file a final report which includes a complete explanation of the incident history, personnel sanctions and/or penalties, resolution status for trend analysis, and reporting for future reference.
	Procedure K: Roles and Responsibilities The CFSA ISO and the Office of Risk Management shall be responsible for maintenance of this policy. The CFSA ISO is responsible for assuring that CFSA workforce members within his or her organizational authority have been made aware of the provisions of this policy, that compliance by the workforce member is expected, and that failure to report information security incidents that impact mission critical, sensitive or confidential information, including Electronic Protective Health Information (EPHI) may result in disciplinary action pursuant to the Sanction Policy.
	Procedure L: Responsibility for Maintenance and Compliance The DSO and CFSA's Security Officer or designee shall be responsible for ensuring that the policy is implemented, enforced and maintained. Compliance by the workforce member is expected, and the unauthorized use of computer network systems, applications, programs and equipment (e.g., PDAs') that receive, store or transmit EPHI data may result in disciplinary action pursuant to the Sanction Policy
	Procedure M: Disciplinary Action for Violations See Sanction Policy.

ATTACHMENT A
DEFINITIONS

For the purpose of This Policy, the definitions have the following meaning:

Incident - Any activity that causes a change in the information security posture of Child and Family Services Agency.

Computer Security Incident - Unexpected, unplanned event that may have a negative impact on information technology (IT) resources, violates security policies, or circumvents security mechanisms, and requires immediate action to prevent further negative impact.

Computer Security Incident Response Team (CSIRT) - A specified group of agency personnel that work with OCTO's DCERT to investigate computer related security events, make incident declaration decisions, and recommend actions during an incident. The activity of CSIRT can be broadly stated as any activity that is related to the identification, containment, eradication, and recovery from any computer security event or incident.

CCB - Change Control Board. A committee that makes decisions regarding whether or not proposed changes to a software project should be implemented. It is used to control identified system changes, review impacts, and grant approvals as part of the change management function that determines the validity and need of (approving or denying) project change requests.

Denial of Service - Prevention of authorized access to resources or the delaying of time-critical operations.

District Computer Emergency Response Team (DCERT) - Pre-established DC Government teams for emergency response to any computer related emergency for the District that interfaces with other District Emergency management teams if required. Normally a DCERT incident requires only one or two persons to investigate. The core DCERT teams are composed of representatives from several key functions and they have the decision-making authority required to take responsive actions during the incident handling process. The function areas include:

1. Anti-Virus
2. DCERT Coordinators
3. Email Operation
4. Intrusion Detection System
5. Network Operations Center
6. OCTO Helpdesk
7. Security Operations
8. VPN
9. WAN Engineering
10. Server Operations

Electronic Media – Is a storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

EPHI - Electronic Protected Health Information: Individually identifiable health information which is transmitted by electronic media and maintained in electronic media. It refers to any information that identifies an individual (usually a patient).

HIPAA - Is an acronym for the Health Insurance Portability & Accountability Act of 1996 (August 21). It mandates the use of standards for the electronic exchange of health care data and to specify what medical and administrative code sets should be used within those standards to require the use of national identification systems for health care patients, providers, payers, or plans. It's a federal act that sets standards for protecting the privacy of personal information.

Mitigation - Reducing or eliminating any potential harm from a security incident.

Security Incident - Event that constitutes administrator/root or user level compromises, malicious logic (i.e., virus, worms, or Trojans) incidents, unsuccessful compromise attempts, denial of service, or scanning/probing incidents. Further, it's defined as an unexpected, unplanned event or activity that may have a negative impact on information technology (IT) resources, violates security policies, or circumvents security mechanisms and requires immediate action to prevent further negative impact.

Workforce - CFSA workforce members includes, but not limited to the following users:

1. Full or part-time employees
2. Contractors who are authorized to use CFSA or District government-owned equipment or facilities
3. Volunteers who are authorized to use CFSA or District government resources and who have been provided with a user account.

ATTACHMENT B

CFSA INFORMATION TECHNOLOGY INCIDENT REPORT FORM

DCERT Ref. #

Date/Time of Incident: **Date/Time of Report:**

Agency: **Address:**

User Info: First Name: _____ Last Name: _____ Phone: _____

Email: _____

User/Host location (if different from Agency address):

ISO/Tech Lead Info: First Name: _____ Last Name: _____ Phone: _____

Email: _____

Incident Type:				
	Misuse/Abuse of Computer Resources	☐	Unauthorized Access	☐
	Computer Virus/Worm/Trojan/ Detection	☐	Suspicious Activity	☐
	Distributed/Denial of Service	☐	Exploit	☐
	Network Availability	☐	Other:	☐

Initial Severity Assigned 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ HIPPA Related? YES ☐ NO ☐

Virus/Worm/Trojan Info: **Removed:** YES ☐ NO ☐

Antiviral Software: **Name:** **Version:** **Date:**

Host Info: Mainframe ☐ Workstation ☐ Server ☐ Network Device ☐ Other ☐ OS:

Source Address	**Port #**	**MAC Address**	**Destination Address**	**Port #**	**MAC Address**

Incident Details

Provide details of events leading up to incident if known, impact on users, details of theft or destruction, and how many users were affected

Action Taken

Name of Person Writing Report: _____

Signature: _____ **Date:** _____

ATTACHMENT C
Child and Family Service Agency
Child Information Systems Administration
Property Release Form

Equipment No.	Device	Manufacturer	Model	Serial No.

By signing this form, you acknowledge and agree that you have received the above mentioned network equipment(s) from the Child and Family Services Agency. You also accept full responsibility for the transportation and safe delivery of the equipment(s) to and/or from the appropriate designation(s).

Name: _____

Office/Department: _____

Telephone Number: _____

CFSA IT Security Officer: _____

Finding	Recommendation	CFSA Reply/Comments
CFSA, DCHR, and DOES do not have policies that govern data collection.	4. District agencies should develop written policies that govern data collection based upon NIST guidelines OR OCTO or another central governmental agency should accomplish this on behalf of all Executive Branch agencies.	CFSA's PII Policy speaks to this recommendation. We are in the process of implementing specific policy defined steps. We have established a Data Collection Committee to assist with the governance of data collection. CFSA will continue to review our established policies based on the National Institute of Standards and Technology (NIST) compliance.
CFSA, DCHR, and DOES do not de-identify PII across all divisions.	5. District agencies, where applicable, should develop written policies and procedures to evaluate how easily the PII they collect can be used to identify specific individuals and de-identify unnecessary information.	CFSA's PII Policy speaks to this recommendation. CFSA is in the process of gathering our data inventory via a request to OCTO and will utilize the results to establish a POA&M for each system. The stakeholders will be contacted for implementation planning.
CFSA and DCHR do not conduct Privacy Impact Assessments.	6. The Mayor should require that all agencies, where applicable, conduct and document a Privacy Impact Assessment or similar assessment to mitigate privacy risks, and post the results of the assessment on their websites.	CFSA will utilize the results of our data inventory to establish a PIA template as part of each systems POA&M, to mitigate our privacy risk.
CFSA, DCHR, and DOES security training was neither consistent nor conducted on an annual basis.	8. The Mayor should direct that all agencies, where applicable, to develop a consistent security training program that is conducted on an annual basis.	CFSA will continue to conduct Security Awareness training for on-boarding and after each FACES training class. We look forward to utilizing the establish DCHR on-line Security training to meet this annual recommendation.

		In addition, we will address the recommendation upon review of CFSA's HIPAA Security Training and Awareness Policy.
CFSA, DCHR, and OCTO have not developed an incident response plan.	11. The Mayor should direct all agencies to adopt and implement a written incident response plan and an incident / breach impact assessment that has been centrally created to address PII.	CFSA is in the process of updating its Incident Response Policy to better define and assess data breaches. The present policy has an established and is in use by the CSIRT team. Based on the policy, with notification from employee, incident reporting and OCTO system generated alerts, we jointly remediate and resolve system and data incidents.

Display Week: 1

TASK	RESPONSIBLE PARTY	Duration (days)	PROGRESS	START	END
1) Conduct Privacy Threshold Analysis/Privacy Assessment Analysis on all systems					
Task 1 - Review Privacy policy (make sure the PTA/PIA processes are mentioned)	Key	1		tbd	tbd
Task 2 - list of inventory (of systems/db)	Suresh/Thirm/OCTO	60		6-27-19	8-26-19
Task 3 - Communicate to stakeholders the PTA/PIA needs	Sylvia/Key/Privacy Officer	5		6-27-19	7-2-19
Task 4- Develop or adopt PTA/PIA templates, if not exist	Key/Sylvia	10		7-2-19	7-12-19
Task 5 - Review and approve the use of template	Sylvia/Privacy Officer	5		7-12-19	7-17-19
Task 6 - Meet with SO/Stakeholders to schedule PTA/PIA activities	Sylvia/Key	15		7-17-19	8-1-19
Task 7 - Assign roles and responsbilities (who to conduct PTA and PIA and who will use the result to do what)	Sylvia/Key/Stakeholders	5		7-17-19	7-22-19
Task 8- Conduct PTA/PIA	Sylvia/Key/Stakeholders	tbd		tbd	tbd
Task 9 - Update privacy records and all privacy related activities if privacy impact changes	Privacy Officer	tbd		tbd	tbd
Task 10 - Post results to CFSA web sites	CIO/Public Affair	tbd		tbd	tbd
2) Implement PII data policies and procedures that govern data collection, handling and exchange:					
Task 1 - Dissiminate the PII policies and procedures to all staff.	OPPPS/Public Affairs Officer	5		5-31-19	6-5-19

Display Week: 1

TASK	RESPONSIBLE PARTY	Duration (days)	PROGRESS	START	END
Task 2 - Review for Implementation	Key/sylvia/OPPPS	10		6-3-19	6-13-19
Task 3 - Contact stakeholders for Implementation	Sylvia/Key	-		6-13-19	tbd
3) Review PII for De-identification implementation					
Task 1- Meet with developers/system owners on how this can be done without much impact	Spencer/Sachin/Key	5		tbd	tbd
Task 2 - Set priorities for systems to be de-identified. (obtain list of systems)	Spencer/Sachin/Key	10		tbd	tbd
Task 3 - Define roles and responsibilities - who to do the de-identification	Spencer/Sachin/Key	10		tbd	tbd
Task 4 - Develop policy or incorporate Deidenfication as requirement for all PII systems in the Data protection policy	Spencer/Sachin/Key	45		tbd	tbd
Task 5 - Develop Standard Operating Procedures	Spencer/Sachin/Key	tbd		tbd	tbd
Task 6 - Launch the Deidentification implementation project for identified systems (Deidentification should be a project for each system on its own)	Sylvia/Key/Spencer	tbd		tbd	tbd
4) Refresh, develop and conduct Security Awareness and Education Training Program					
Task 1 - Define roles and responsibilties	Sylvia/Key/CWTA/Privacy Officer	5		tbd	tbd
Task 2 - Review, refresh and update the Cyber Security Awareness and Education Training curriculum (CSAT) for all workforce members	Sylvia/Key/CWTA/Privacy Officer	15		tbd	tbd

Display Week: 1

TASK	RESPONSIBLE PARTY	Duration (days)	PROGRESS	START	END
Task 3 - Communicate to all workforce members of the CSAT schedule	Public Affair	5		tbd	tbd
Task 4 - Conduct the CSAT according to schedule	Sylvia/Key/CWTA/Privacy Officer	tbd		tbd	tbd
Task 5- Report results to District government	Sylvia/Marina	tbd		tbd	tbd
5) Review/update and implement Incident Response Plan					
Task 1 - Review existing IRP for data intergity and breach notification	Key	2		15-05-19	17-05-19
Task 2 - Incorporate IRP information into the CSAT curriculum	Sylvia/Key/CWTA/Privacy Officer	5		24-06-19	29-06-19
Task 2 - Schedule quarterly meeting with CISRT team	Sylvia/Key	2		29-06-19	01-07-19
Task 3 - Conduct plan review (including the communication plan and the COOP plan)	Key	10		01-07-19	11-07-19
Task 4 - Test the IR Plan by scheduling and conducting a quarterly table top exercise	Key	5		tbd	tbd
Task 5 - Post testing review/Lesson Learned	Key	5		tbd	tbd
Task 6 - Documentation/Update	Key	10		tbd	tbd
Task 7 - Plan Maintenance	Sylvia/Key	5		tbd	tbd

Office of the Director

May 20, 2019

Kathleen Patterson, DC Auditor
717 14th Street, NW
Suite 900
Washington, DC 20005

Subject: **DCHR Response to D.C. Auditor Report, "Some Progress But More Improvement Needed In Management of Personally Identifiable Information"**

Dear Ms. Patterson:

The Office of the District of Columbia Auditor ("ODCA") released a report on January 6, 2017 entitled, "The D.C. Government Must Improve Policies and Practices for the Protection of Personally Identifiable Information" ("2017 D.C. Auditor Report"). The 2017 D.C. Auditor Report identified concerns ODCA had regarding the District's management of Personally Identifiable Information ("PII") and ways in which ODCA believed District government, including the D.C. Department of Human Resources ("DCHR"), should seek to improve the protection of PII. After reviewing the newest report entitled, "Some Progress But More Improvement Needed In Management of Personally Identifiable Information" ("2019 D.C. Auditor Report"), DCHR is encouraged to see that ODCA has recognized the progress DCHR has made since the 2017 D.C. Auditor Report. DCHR offers the following response and explanation of the steps taken to date, as well as the steps that DCHR plans to take in the future to ensure the continued protection of PII.

Progress in the Protection of PII

After the release of the 2017 D.C. Auditor Report, DCHR began to implement improvements in the protection of PII to address the various recommendations provided in the report. Some of those improvements are highlighted in the 2019 D.C. Auditor Report. The following are several of the major improvements DCHR is most proud of.

First, DCHR ensured that 100% of its employees completed the Office of the Chief Technology Officer's ("OCTO") online Cybersecurity Training, which included a segment on PII. Second, DCHR collaborated with OCTO to ensure that Peoplesoft, the District government's Human Resources Management Information System, is an encrypted system. Third, DCHR successfully implemented Secure Print, a process that requires employees to use their badges to print any document, including documents that contain PII, from printer/copier machines. Moreover, DCHR uses the mobile device platform (MDM) VMware AirWatch, which allows IT staff to control, secure and enforce policies on smartphones, and tablets. ZixEncrypt assists in the reduction of PII loss via content filtering, protecting email and sensitive information by making email encryption to anyone on any device.

Additionally, the Standard Form 50, one of DCHR's key forms used to record personnel actions, was modified to only display the last four digits of a person's Social Security number when printed. DCHR has also installed encryption on all agency laptops using BitLocker, a full volume encryption application. Lastly, DCHR has successfully complied with the District of Columbia Data Policy which, among other things, requires all agencies to create and maintain an inventory all datasets and classify them by level of sensitivity.

Next Steps

DCHR appreciates ODCA's acknowledgment of the improvements we have undertaken since the publication of the 2017 D.C. Auditor's report. However, DCHR is seeking ways to build upon those improvements. For example, we are exploring how best to conduct both a Privacy Threshold Analysis and Privacy Impact Assessment. DCHR is also exploring options for updating its Administrative Order entitled "Personally Identifiable Information (PII) and Personnel Records," dated October 1, 2018, to align more with the recommendations provided in the 2019 D.C. Auditor Report. Updates to the Administrative Order may include:

- a more formal process for eliminating unneeded PII collection;
- procedures for data collection based upon NIST or OCTO guidelines;
- an alignment of DCHR's Incident Response Plan with OCTO's Cyber Security Incident Response Team Policy; and
- procedures for PII de-identification.

DCHR will train its employees on the content of the Administrative Order. Further, DCHR will ensure that every employee completes training by requiring mandatory attendance and requiring each employee provide proof of completion. DCHR will also distribute the Administrative Order to all employees and require each employee to sign an acknowledgment of receipt.

Conclusion

DCHR thanks ODCA for its assessment of how PII is protected by the District government and its acknowledgment of the steps DCHR has taken to improve its protection and security of PII. Additionally, DCHR appreciates the opportunity to respond to ODCA's latest report, "Some Progress But More Improvement Needed In Management of Personally Identifiable Information." As a District agency entrusted with sensitive employee information, we take seriously our responsibility to protect this information and will continue to evaluate and improve our use and maintenance of PII.

Sincerely,

Ventris C. Gibson
Director, D.C. Department of Human Resources

GOVERNMENT OF THE DISTRICT OF COLUMBIA

Department of Employment Services

MURIEL BOWSER
MAYOR

DR. UNIQUE MORRIS-HUGHES
DIRECTOR

May 24, 2019

Kathleen Patterson
District of Columbia Auditor
Office of the District of Columbia Auditor
717 14th Street, NW
Washington, DC 20005

Dear Ms. Patterson:

On behalf of the Department of Employment Services, I hereby submit this information in response to your draft audit report dated May 6, 2019 titled ***Some Progress But More Improvement Needed In Management of Personally Identifiable Information.***

Regarding page number 7of the draft report, under ***What We Found at the Agencies: DOES***, ODCA cited the following:

> *DOES has two policies, Handling Sensitive Information and Data Integrity, that collectively cover different aspects of proper PII management and safeguarding. One of these policies was in existence when we published our January 2017 report and one has been updated since that time. Neither, however, address collecting PII data. According to DOES officials, all staff have been notified of the existence of these policies and are provided with training on proper PII management. However, the training demonstrated was an online tutorial that staff were expected to take by themselves. After reviewing this tutorial, it was not clear that it related directly to DOES's own policies and procedures. Instead, it appeared to cover PII management from a generic perspective. Further, DOES did not provide documentation demonstrating that these trainings have taken place.*

DOES acknowledges the concerns noted above and is committed to building a more robust and compliant means by which PII is collected and safeguarded. DOES currently has global PII safeguarding processes in place. In step with methodologies delineated in the National Institute of Standard and Technology issued by the United States Department of Commerce, DOES will impose the following updates and enhancements to our existing PII policies, processes, and procedures:

1. Update DOES policy *600.30-2 – Handling Sensitive Information* to include PII requirements and best practices by Fiscal Year 2020 (FY20);

2. Update DOES policy *DOES-SEC-009 – Data Integrity* to incorporate PII requirements and best practices by FY20;

3. Develop and/or enhance as applicable, DOES bureau-specific operational procedures, as well as initial and refresher training tools that includes PII handling requirements, in alignment with enhanced governing policies (Handling Sensitive Information and Data Integrity);

4. Mandate a 100 percent requirement for distribution of revised policies, processes, and procedures to all DOES managers and staff;

5. Mandate a 100 percent requirement for initial and refresher training requirement for all DOES managers and staff;

6. Repurpose the online PII tutorial as a secondary, but required, training tool to be utilized each time a new system access is requested by DOES managers or staff; and

7. Begin distributing and training DOES managers and staff on newly implemented policies, processes, and procedures by FY20.

Regarding page number 10 of the draft report, under ***Encryption: DOES***, ODCA cited the following:

> *DOES officials explained the difficulties they face in encrypting databases. To do so would result in unacceptable loss of efficiency in doing their day-to-day work as their systems would become too slow in attempting to access the encrypted data. Instead, they explained, they are looking at encrypting only those data tables or other elements that contain PII, which will reduce the data processing load. Because some of their data resides on servers controlled by OCTO, DOES officials were not sure whether they could accomplish full integration without OCTO's help.*
>
> *DOES's Data Integrity Policy requires end-user storage devices with PII to be encrypted. Officials from the agency further explained and demonstrated that those division within the agency where PII would often or usually need to be displayed on computer screens or otherwise used at employees' desks are in secure portions of their building. Entry into these offices is controlled and inly authorized personnel may gain access.*

DOES acknowledges this as an accurate representation of current challenges and work-arounds applied by DOES to ensure the safeguarding of PII.

Thank you for the opportunity to address the concerns and notations cited in the ODCA draft audit report. Should you or your team have any questions regarding this submission, please contact Ramon Perez-Goizueta, Chief Compliance Officer at (202) 671-1673 by phone or Ramon.Perez-Goizueta2@dc.gov by email.

Sincerely,

Unique Morris-Hughes
Director

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

May 20, 2019

Ms. Kathleen Patterson
DC Auditor
717 14th Street, NW, Suite 900
Washington, DC 20005

Dear Ms. Patterson:

The Office of the Chief Technology Officer (OCTO) is in receipt of your report entitled "Some Progress But More Improvement Needed In Management of Personally Identifiable Information." As you know, the DC Government is a unique form of government, providing services that cities, counties and states provide all from within one municipality. Given that perspective, there are many different types of Personally Identifiable Information (PII) collected by the government, and while a one size fits all policy approach might work for a municipality just serving a state function or just serving a city function, ours requires a significantly more nuanced approach. As we learned at a recent conference attended by the state CIOs, no states have yet promulgated a comprehensive PII policy that allows for the needed controls, and yet needed flexibility to use data to serve people efficiently and effectively.

Efficiently serving people often requires sharing data across agencies. While preserving and protecting PII is critical, facilitating the secure sharing of data across agencies is also a key focus of OCTO. OCTO will continue to collaborate with other DC Government agencies in its efforts to maintain a robust infrastructure and ensure that PII is securely protected while being collected, analyzed, stored and shared.

- OCTO is committed to continuing to comply with existing federal statutes and regulations that address the collection, transmittal, storage and de-identification of PII.

- OCTO is committed to continuing to comply with the April 27, 2017 Mayor's Order 2017-115, "District of Columbia Data Policy," which identified two roles within OCTO to manage, protect and secure PII, including a Chief Data Officer (CDO) as the senior official responsible for the District's data governance processes and a Chief Information Security Officer (CISO) as the senior official responsible for providing oversight of the security of the District's information technology infrastructure and networks.

- OCTO assisted 75 agencies to record a total of 1,779 enterprise datasets, making it easier to assess the nature of the data held by each agency and determine whether it contains PII, and thus is not subject to public disclosure.

- OCTO annually implements a District-wide cybersecurity awareness training program, conducted in conjunction with the Department of Human Resources.

- OCTO continues to establish a cybersecurity policy framework consistent with the National Institute of Standards and Technology (NIST), including incident response protocol.

OCTO will continue to lead and improve the District's handling of PII, as we collectively seek to protect the identities and information entrusted to the DC Government by residents, businesses and visitors.

Sincerely,

Lindsey V. Parker
Chief Technology Officer

Auditor's Response to Agency Comments

We appreciate the responses to our draft report provided by OCTO, CFSA, DOES, and DCHR.

We are encouraged by DCHR's plans to explore how best to conduct both a Privacy Threshold Analysis and Privacy Impact Assessment, as well as its efforts to update its PII policy and bring it closer into alignment with the recommendations we made in our January 2017 report. We are gratified to learn that CFSA has taken steps to improve its Incident Reporting policy, reportedly done, in part, because of our involvement.

DOES also has reported several actions it will be taking to enhance its existing PII policies and procedures to bring them closer to National Institute of Standards and Technology standards. We appreciate that DOES recognizes in its response that our description of their efforts at encryption so far are "an accurate representation of current challenges and work-arounds applied by DOES to ensure the safeguarding of PII."

OCTO indicated in its letter that it is "committed" to continuing to comply with existing federal statutes and regulations, including the District of Columbia Data Policy. OCTO also wrote that "while a one-size-fits-all policy approach might work for a municipality just serving a state function or just serving a city function, ours requires a significantly more nuanced approach." While we appreciate the unique challenges in governance faced by agencies in the District of Columbia, we trust that OCTO also will continue its pursuit of a District-wide PII policy applicable to all Mayoral agencies, as described to us in numerous interviews with high-level agency officials. These same officials have stressed to us that a single set of basic standards is critical to minimizing the risk of cyberattacks in the District government and that agencies would be free to add to this basic policy in ways that would address their special needs.

We look forward to OCTO's collaboration with the Executive Office of the Mayor on legislation to strengthen and clarify the authority OCTO has to oversee and direct the management of risks associated with collecting and managing PII throughout the District government.

Appendix A

Findings and Recommendations from ODCA's January 2017 Report on PII Management by the District of Columbia Government

Finding	Recommendation
The District government lags behind the private sector in protection of PII because it lacks a central governmental IT authority.	**1.** The Mayor should designate a central governmental entity with sufficient executive authority to carry out District-wide IT security functions and establish policies and procedures.
The District does not have government-wide policies and procedures for documenting the identification of PII it collects.	**2.** The Mayor should designate a central governmental agency to document all PII that is collected and stored across all District agencies. **3.** The Mayor should require that every agency, where applicable, conduct and document a Privacy Threshold Analysis and publish the results on its website.
CFSA, DCHR, and DOES do not have policies that govern data collection.	**4.** District agencies should develop written policies that govern data collection based upon NIST guidelines OR OCTO or another central governmental agency should accomplish this on behalf of all Executive Branch agencies.
CFSA, DCHR, and DOES do not de-identify PII across all divisions.	**5.** District agencies, where applicable, should develop written policies and procedures to evaluate how easily the PII they collect can be used to identify specific individuals and de-identify unnecessary information.
CFSA and DCHR do not conduct Privacy Impact Assessments.	**6.** The Mayor should require that all agencies, where applicable, conduct and document a Privacy Impact Assessment or similar assessment to mitigate privacy risks, and post the results of the assessment on their websites.
Sampled agencies have written PII confidentiality policies and procedures but these policies are not always comprehensive, consistent across agencies or distributed to relevant employees.	**7.** The Mayor should designate a central governmental IT agency to develop, distribute, and monitor agency-wide PII confidentiality policies and procedures.
CFSA, DCHR, and DOES security training was neither consistent nor conducted on an annual basis.	**8.** The Mayor should direct that all agencies, where applicable, to develop a consistent security training program that is conducted on an annual basis.

DCHR and DOES do not require that all end user storage devices be encrypted.	**9.** The Mayor should require that all District-issued laptops and USBs that maintain PII area encrypted.
Not all DCHR and DOES databases are encrypted.	**10.** The Mayor should direct that all agencies encrypt databases that contain PII or employ some other method to minimize the amount of PII data that can be accessed.
CFSA, DCHR, and OCTO have not developed an incident response plan.	**11.** The Mayor should direct all agencies to adopt and implement a written incident response plan and an incident / breach impact assessment that has been centrally created to address PII.

About ODCA

The mission of the Office of the District of Columbia Auditor (ODCA) is to support the Council of the District of Columbia by making sound recommendations that improve the effectiveness, efficiency, and accountability of the District government.

To fulfill our mission, we conduct performance audits, non-audit reviews, and revenue certifications. The residents of the District of Columbia are one of our primary customers and we strive to keep the residents of the District of Columbia informed on how their government is operating and how their tax money is being spent.

Office of the District of Columbia Auditor
717 14th Street N.W.
Suite 900
Washington, DC 20005
Call us: 202-727-3600
Email us: odca.mail@dc.gov
Tweet us: https://twitter.com/ODCA_DC
Visit us: www.dcauditor.org

Office of the District of Columbia Auditor