Office of the District of Columbia Auditor

FOR IMMEDIATE RELEASE
January 6, 2017
View the full report

Contact: Diane.Shinn@dc.gov
202-727-8991

D.C. Must Improve Protection of Personal Information

Report shows IT authority is needed to set & monitor policies and procedures to protect privacy

WASHINGTON, D.C.—While the District has made progress in protecting the vast amount of personally identifiable information (PII) it collects and stores, District-wide inconsistencies in policies and procedures for documenting, maintaining and protecting PII leave the District's stockpile of PII vulnerable to cyberattacks and security breaches, according to a new report by the D.C. Auditor.

"It is incumbent upon the District to ensure that it has airtight internal controls over all PII it collects and stores, and that we have consistent confidentiality policies and procedures in place across all agencies to protect the privacy of those individuals who have entrusted us with their sensitive personal information," said D.C. Auditor Kathy Patterson. "This report shows that the District government is not doing everything it can to protect PII, mainly because it lacks District-wide oversight of security functions and centralized policies and procedures governing PII."

The National Institute of Standards and Technology defines PII as any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name or biometric records, including fingerprints, handwriting, etc.

Since 2007, the D.C. Office of the Inspector General (OIG) has issued 17 reports that included findings in which District agencies were not properly safeguarding PII. The OIG report, together with massive data breaches in the federal government—including the June 2015 discovery that highly sensitive information from the U.S. Office of Personnel Management—including SSNs of some 21.5 million individuals—had been stolen, prompted the review of internal controls over PII in the District government, ODCA's report said.

The ODCA report specifically cites wide variations in how District agencies:

- De-identify records so that enough PII is removed or obscured leaving information that cannot identify an individual.
- Determine risks and effects of collecting, maintaining, and disseminating PII in identifiable form, and identify and evaluate protections and alternative processes for handling PII to mitigate potential privacy risks.
- Develop, distribute, and monitor agency-wide PII confidentiality policies and procedures and incidence response plans, including restrictions on sharing of PII and requirements for notification to all parties in the case of a breach.
- Develop and conduct security training consistently across all agencies on an annual basis.
- Encrypt databases and digital storage devices containing PII to add an additional layer of protection requiring access to a secret key or password that enables the review of PII.

Based on those findings, the report's primary recommendation is that the District designate a central agency with the executive authority to conduct District-wide IT security functions and direct that agency to develop, distribute and monitor all PII confidentiality policies and procedures.

The report describes the current role of the Office of the Chief Technology Officer (OCTO) as providing general directives regarding PII policies and procedures, but notes that the agency neither monitors the PII policies and procedures developed by other District agencies nor does it track whether all agencies have policies and procedures to protect PII. The report notes that when OCTO was created it provided IT direction across the District government, but over time the agency's authority has been diminished.

According to guidelines set forth by the GAO Executive Guide on Information Security Management, the District will not be able to spot trends, fully identify problem areas, and ensure that policies and administrative actions regarding PII are handled properly without centralized management and oversight of IT security and protection of PII.

In a written response included in the published report, the Office of the Chief Technology Officer (OCTO) generally concurred with the goals and plans to adopt ODCA's 10 recommendations. In its response to OCTO, ODCA acknowledges that the administration has already begun implementing some of the report's recommendations, particularly that they have expanded the role and scope of the newly hired Chief Information Security Officer, and have hired a Governance, Risk and Compliance manager to proactively improve policies, access and control risk, conduct internal compliance assessments, and coordinate support for external audits for OCTO and other agencies.

Other ODCA recommendations include:

- Direct a central agency to document all PII that is collected and stored District-wide.
- Require all agencies to develop and conduct annual security training programs.
- Direct all agencies to ensure that all agency-issued laptops and USBs that maintain PII are encrypted.
- Require all agencies to encrypt databases that contain PII or ensure that a minimum of PII data can be accessed via databases.
- Direct that all agencies develop a written incident response plan and an incident/breach impact assessment that address PII.

View the full report.

# # #

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. Learn more at www.dcauditor.org.