March 2023 DC Health Link Data Breach
Testimony of Catherine L. Szpindor
Chief Administrative Officer

April 19, 2023
2:00 PM

Before:
House Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation
&
Committee on House Administration Subcommittee on Oversight

Thank you, Chairwoman Mace, Chairman Loudermilk and Ranking Members Torres and Connolly as well as the other Members of the House Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation and the Committee on House Administration Subcommittee on Oversight.

I appreciate the opportunity to testify before the subcommittees to discuss the data breach involving DC Health Benefit Exchange Authority's online healthcare exchange system – DC Health Link. The details and timeline specific to the data breach described in this testimony include information as reported to the Office of the Chief Administrative Officer (CAO).

As the Subcommittees are aware, the DC Health Link system is independently operated by the District of Columbia Government. The CAO's relationship with DC Health Link is compulsory in nature and is limited to the secure exchange of information required to facilitate House participation in healthcare programs as required by the Patient Protection and Affordable Care Act (ACA), effective January 1, 2014, and subsequent Office of Personal Management (OPM) rulings pertaining to the law's implementation. Though the CAO has and will continue to participate in incident briefings that include the U.S. Capitol Police, the DC Health Link operators, and House Leadership, it does not operate nor have involvement in the security measures used to protect the DC Health Link system.

By way of background, the House's information-sharing relationship dates back to 2013 when Members and staff first enrolled in DC Health Link healthcare programs for calendar year 2014. The enrollment process starts when the CAO adds Members and staff eligible to enroll in healthcare plans to the DC Health Link system via an administrative portal. Once added, Members and staff receive a notice from the CAO with enrollment instructions.

Each month, DC Health link and the CAO follow an established secure data transfer protocol to pay healthcare premiums, report terminations, and fix information discrepancies. DC Health Link transfers Member and staff healthcare plan premium costs to the CAO to facilitate payment of the employer contribution and deduct the employee portion of the premium from individuals'

monthly pay. Using the same protocol, the CAO provides DC Health Link with House employment termination reports, and both entities transfer what are known as "issue logs," which are lists of identified account discrepancies that require resolution.

The secure data transfer protocol is outlined and solidified between the two entities in an interconnection security agreement. Both entities have also entered into a standard trading partner agreement to ensure the integrity, security, and confidentiality of the data electronically exchanged. The two agreements require DC Health Link to conform to all applicable DC and federal laws, rules, regulations, and policies governing the privacy and security of data exchanges.

The secure data exchange protocol used for transfers between the CAO and DC Health Link is like other compulsory interagency data exchanges the CAO facilitates for Member and staff benefit administration, including healthcare plans provided by OPM and the Thrift Savings Plans program. The CAO is required to withhold federal, state, and employer taxes for over 10,000 individuals, which requires the secure exchange of personal identifiable information (PII) with U.S. Treasury, Social Security Administration, and every state taxation or treasury department.

All the federal and state entities that the CAO shares Member and staff data with, including the DC Health Benefit Exchange Authority, are required to comply with federal and applicable state security requirements as well as their own internal agency requirements. And every institution – public and private – must contend with the growing and ever-evolving threats posed by cyber criminals. Those safeguarding individuals' PII have an even greater challenge.

As the entity responsible for safeguarding the U.S. House and its Members against billions of attempted cyber threats and probes each year, the CAO can attest to the extremely challenging landscape each institution must navigate. The CAO has worked hard to establish and execute secure data sharing protocols with all its partners, including the DC Health Benefit Exchange Authority. And it will continue to ensure the integrity of that relationship. However, once data is securely transferred to another entity, the CAO's jurisdiction ends. The CAO does not validate, nor can it mandate the security measures of other government entities with which it is required to interface.

As evidenced by the breach, DC Health Link appears to have had some unresolved security matters. In addition to assistance provided by the CAO, U.S. Capitol Police, and the Federal Bureau of Investigation, it is the CAO's understanding that the DC Health Benefit Exchange Authority has procured services from a reputable cyber security firm that will greatly assist in the investigative and remediation efforts.

And although the CAO cannot investigate nor dictate internal security measures employed by the DC Health Benefit Exchange Authority for DC Health Link, it certainly can and will ensure the House community is informed about incidents if and when they occur and advocate for the House to receive needed protections that mitigate fraud and damage as was the case with the DC Health Link breach.

Upon learning about the DC Health Link breach late morning Tuesday, March 7, 2023, the CAO cyber team, which already monitors the House network 24/7/365, confirmed none of the servers nor applications supported by the House had been compromised. Simultaneously, CAO management worked with the DC Health Benefit Exchange Authority, U.S. Capitol Police, and the House Sergeant at Arms to understand the scope of the breach and what, if any, House information was involved. By the end of the day, it was confirmed that House information maintained by DC Health Link was in fact compromised and the CAO was provided a copy of the data. Once it received the compromised data, the CAO's Payroll and Benefits team validated the data. Note that House DC Health Link enrollees commonly use personal email addresses when enrolling that lack unique identifiers. The compromised data was also scrubbed of all PII before being provided to the CAO. Therefore, individuals' data included in the confirmed compromised data needed to be accurately validated using other identifiers. It was critical the CAO have a 100 percent accurate accounting of those impacted.

After confirming Member and staff PII data was compromised, the CAO sent a series of communications. First it sent communications to the potential universe of impacted individuals and then to the confirmed universe of impacted individuals.

Working with House Leadership, on March 8, 2023, while validating the data it received, the CAO sent communications to all individuals whose information could have been compromised – meaning all Members and staff deemed eligible for healthcare through DC Health Link. All were encouraged to freeze their and their family's credit at the three major credit bureaus out of an abundance of caution. They were also provided with additional steps individuals should take to avoid becoming a victim of financial fraud.

On March 9-10, 2023, once the data was validated and investigators and the CAO had a clearer picture of the scope of the breach, the CAO sent additional communications. Communications were sent to House Members and staff whose information was confirmed to have been compromised as well as to Members and staff whose information was confirmed not to have been compromised at that point of the investigation. All were provided instructions on how to obtain free credit and identity monitoring services. Notices were also sent to impacted individuals no longer employed by the House but whose information was confirmed to have been included in the breach.

The CAO also participated in separate briefings for Members and staff hosted by the Committee on House Administration and included regular important breach updates in Payroll and Benefits newsletters distributed House-wide. The CAO Payroll and Benefits Team has and continues to field calls from the House community pertaining to the breach.

The investigation into the breach, its scope, and its impact on the House community is still underway. Since learning about the breach, House Leadership, the U.S. Capitol Police, the House Sergeant at Arms, and CAO's cyber team were quick to respond and highly instrumental

in mitigating damage. For example, with the support of House Leadership, everyone in the House community – past and present – ever considered eligible for healthcare via DC Health Link, is eligible for three years of free credit and identity monitoring services paid for by DC Health Link.

This incident, like the 2015 OPM breach, is a sobering reminder of why cybersecurity is the top priority for the CAO. Each year, the CAO deploys over a quarter million software patches, protects more than 3,000 servers, and stops tens of millions of attempted cyber-attacks and billions of attempted probes. It rigorously vets on-premises and cloud applications used by the House community.

For clarification, the on-premises and cloud applications used by the House are discretionary, unlike systems operated by other government entities with which the CAO has a compulsory relationship. The CAO has the authority to validate, test, and even demand specific security protocols prior to authorizing the use of discretionary applications.

The CAO has made great progress in its efforts to protect the House and its users from cyber threats. In fact, a third-party cyber maturity assessment originally conducted in 2017 and again in 2022 shows significant improvements in cyber governance, human compliance, information risk management, business continuity, operations and technology, and legal compliance and auditing. With the support of House Leadership, the CAO addressed staffing deficiencies and significantly increased capabilities – most of which are behind-the-scenes improvements to include enhanced, real-time network monitoring, better malware detection tools, and improved security controls over devices and applications.

The CAO has also implemented improvements the House community sees, like disabling USB drives throughout the House, sending timely warnings about current email phishing campaigns, and deploying cyber pop-ups around campus to engage and inform staff. All staff participate in our required annual cyber training. We require IT support providers to patch various operating systems to remain compliant. The CAO notifies offices when a vendor is noncompliant, and requests immediate action be taken. On several occasions, the CAO has blocked vendors' access to the network and terminated their contracts.

It takes tremendous time, discipline, and resources to protect the House's IT infrastructure and data. The House's technology environment is distributed across Member offices here in Washington DC and across the country in nearly a thousand district offices. Some offices, Member and committee, employ technology support staff not under the purview of the CAO.

Strong cybersecurity requires consistent, strict adherence to security practices and training – by *every* member of the House community. The CAO recognizes that its requirements are not always popular with Members and staff, but this breach underscores the reason we need them. The House is a target. If we are not vigilant, the CAO could also suffer a significant data breach.

We can never accept the status quo and must always remain a step ahead. As CAO, I spend considerable time and effort working with my staff to ensure we are securing House data. In my opinion, the CAO has, and will always have, a tremendous amount of work to do. And we will continue to work with the Committee on House Administration, House Leadership, and all of our stakeholders to make sure we have the right policies and capabilities in place to ensure we protect House data and are prepared to address security issues should they ever arise.

Again, the CAO appreciates the opportunity to testify before the subcommittees and discuss the data breach involving DC Health Link operated by the DC Health Benefit Exchange Authority. We look forward to working with the subcommittees and our other Legislative Branch partners as this investigation continues.