HOUSE OFFICER PRIORITIES FOR 2019 AND BEYOND

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

_____

APRIL 9, 2019

_____

Printed for the use of the Committee on House Administration

❈

C O N T E N T S

_____

APRIL 9, 2019

HOUSE OFFICER PRIORITIES FOR 2019 AND BEYOND

TUESDAY, APRIL 9, 2019

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The Committee met, pursuant to call, at 10:01 a.m., in Room 1310, Longworth House Office Building, Hon. Zoe Lofgren [Chairperson of the Committee] presiding.

Present: Representatives Zoe Lofgren, Raskin, Mrs. Susan Davis of California, Butterfield, Fudge, Aguilar, Mr. Rodney Davis of Illinois, Mark Walker, and Barry Loudermilk.

Staff Present: Sean Jones, Legislative Clerk; Khalil Abboud, Deputy Staff Director; Teri Morgan, Deputy Staff Director; David Tucker, Parliamentarian; Daniel Taylor, Chief Counsel; Jamie Fleet, Staff Director; Peter Whippy, Communications Director; Brittany Randall, Minority Director of Member Services; Timothy Monahan, Minority Director of Oversight; Jennifer Daulby, Minority Staff Director; and Courtney Parella, Minority Communications Director.

The CHAIRPERSON. The Committee on House Administration will come to order. I would like to thank the Members of the Committee, our witnesses, and all those in the audience for being here today.

I am pleased to have our House officers with us this morning.

The work you perform enables us to keep focused on our work, delivering for our constituents, and we are grateful for it.

House operations face many challenges. Physical and cyber security, both here and in our districts and attracting and retaining a highly skilled, diverse workforce and helping Member offices adopt new technologies that allow all of use to communicate better with our constituents is so important.

These challenges and many more require us to be constantly re-evaluating what works and what doesn't and to be always planning and prioritizing based on the highest value for the taxpayer and the greatest service for the Member office.

It is my intention to continue the tradition of this Committee with bipartisan work on overseeing our House officers. I know Mr. Davis' staff and mine meet regularly with each of you on ongoing projects and initiatives. And I believe the House works better when more opinions are heard about how it should work. Our hearing this morning is the first of many to make sure that we are meeting our responsibilities as stewards of this great institution.

Before we begin, I would like to make a couple of comments about the men and women who work with the House officers and Inspector General. From the tally clerks to the security engineers, the protocol officers and the financial statement auditors, this Com-

mittee will focus on making sure that every institutional office of the House is a good place to work, where people are treated fairly and with respect.

In the near future, we will restart our workplace rights training. I have reviewed every page of the curriculum, incorporating feedback from Members and staff alike, to make sure it works with our new House Rules. We are also working with our vendor to find ways we can make the training more meaningful for managers and supervisors who are on the front lines of creating a welcoming workplace.

I would like now to recognize our Ranking Member, Mr. Davis, for any opening remarks that he may wish to make.

[The statement of the Chairperson follows:]

STATEMENT OF CHAIRPERSON ZOE LOFGREN, COMMITTEE ON HOUSE ADMINISTRATION HEARING, "HOUSE OFFICER PRIORITIES FOR 2019 AND BEYOND.", APRIL 9, 2019

The Committee on House Administration will come to order. I would like to thank the Members of the Committee, our witnesses, and all those in the audience for being here today.

I'm pleased to have our House Officers and Inspector General with us this morning. The work you perform helps enables us to keep focused on our work—delivering for our constituents and we are grateful for it.

House operations face many challenges: physical and cyber security, both here and in our districts, attracting and retaining a highly skilled, diverse work force and helping Member offices adopt new technologies that allow all of us to better communicate with our constituents. These challenges—and many more—require us to be constantly re-evaluating what works and what doesn't and to be always planning and prioritizing based on the highest value for the taxpayer, and the greatest service for the Member office.

It is my intention to continue the tradition of this Committee with bipartisan work on overseeing our House Officers. I know Mr. Davis' staff and mine meet regularly with each of you on ongoing projects and initiatives and I believe the House works better when more opinions are heard about how it should work.

Our hearing this morning is the first of many to make sure we are meeting our responsibilities as stewards of this great institution.

Before we begin I'd like to make a couple of comments about the men and women who work for the House Officers and Inspector General. From the tally clerks, to the security engineers, the protocol officials and the financial statement auditors, this Committee will focus on making sure that every institutional office of the House is a good place to work, where people are treated fairly and with respect.

In the near future we will restart our workplace rights training. I've reviewed every page of the curriculum incorporating feedback from Members and staff alike, and making sure it works with our new House Rules.

We are also working with our vendor to find ways we can make the training more meaningful for managers and supervisors, who are on the front lines creating a welcoming workplace.

I now recognize the Ranking Member for any opening remarks that he may wish to make.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

Welcome to our officers.

Before I begin, I would like to take a minute, though, to recognize and honor the contributions made to the House by two individuals, Alan DeLuca and Mike Pratt. Both these men were longtime employees of the CAO who recently passed away. And it is the tireless work ethic and steadfast commitment to service that Mike and Alan both demonstrated that make our jobs as Members of Congress much easier. My deepest sympathies are extended to their families and their friends and all their coworkers.

The Chief Administrative Officer, Mr. Kiko—great to see you—Clerk and House Inspector General and their teams are collectively responsible, as we know, for the non-political operations of the House. They are tasked with authenticating the legislative process, through the Clerk's operation; managing the business processes that allow every office to function, through the CAO's operation; ensuring every Member, staffer, and visitor has a safe experience, through the Sergeant at Arms administration; and then through the watchful eye of the Inspector General, their operation, all of those tasks and processes are reviewed to ensure that taxpayer dollars are spent wisely.

All of you have laid out important priorities for the 116th Congress in your testimony, from modernizing the Legislative Information Management System, to improving physical security in district offices, to enhancing cyber-security for the House. It is clear your priorities are thoughtful and intended to improve House operations.

There is a constant balance between the priorities of the institutional offices and the priorities of Member offices who rely on their services to operate. The priorities of both are often in alignment, but at times there is a disconnect between what institutional offices think Member offices need versus what they need.

My overarching priorities for all four of you do can be broken into four areas: first, improving proactive communication with offices; second, building a strong culture of service in all that you do; third, instituting commonsense processes and procedures—we don't need to make things overly bureaucratic just because we can—and, finally, ensuring the House is getting a return on investment for the additional resources that you receive. With additional resources also come additional expectations.

Thank you all for being here today. I look forward to working with you, continuing to work with each one of you.

I yield back.

[The statement of Mr. Davis of Illinois follows:]

STATEMENT OF RANKING MEMBER RODNEY DAVIS, COMMITTEE ON HOUSE ADMINISTRATION HEARING, "HOUSE OFFICER PRIORITIES FOR 2019 AND BEYOND.", APRIL 9, 2019

Before I begin, I would like to take a minute, though, to recognize and honor the contributions made to the House by two individuals, Alan Deluca and Mike Pratt. Both of these men were longtime employees of the CAO who recently passed away. And it is the tireless work ethic and steadfast commitment to service that Mike

and Alan both demonstrated that make our jobs as Members of Congress much easier. My deepest sympathies are extended to their families and their friends and all their co-workers.

The Chief Administrative Officer, Sergeant at Arms, Clerk, and House Inspector General and their teams are collectively responsible, as we know, for the non-political operations of the House. They are tasked with authenticating the legislative process, through the Clerk's operation; managing the business processes that allow every office to function, through the CAO's operation; ensuring every Member, staffer, and visitor has a safe experience, through the Sergeant at Arms administration; and then through the watchful eye of the Inspector General, their operation, all of those tasks and processes are reviewed to ensure that taxpayer dollars are spent wisely.

All of you have laid out important priorities for the 116th Congress in your testimony, from modernizing the Legislative Information Management System, to improving physical security in district offices, to enhancing cyber-security for the House. It is clear your priorities are thoughtful and intended to improve House operations.

There is a constant balance between the priorities of the institutional offices and the priorities of Member offices who rely on their services to operate. The priorities of both are often in alignment, but at times there is a disconnect between what institutional offices think Member offices need versus what they actually need. My overarching priorities for all that the four of you do can be broken into four areas.

First, improving proactive communication with offices. Second, building a strong culture of service in all that you do. Third, instituting common sense processes and procedures—we don't need to make things overly bureaucratic just because we can. And, finally, ensuring the House is getting a return on investment for the additional resources that you receive. With additional resources also come additional expectations.

Thank you all for being here today. I look forward to working with each of you and your organizations. I yield back.

The CHAIRPERSON. Thank you, Mr. Davis.

Joining us today is Cheryl L. Johnson, the Clerk of the House. Ms. Johnson was sworn in as Clerk of the House on February 25, 2019 and is the 36th individual to serve as our Clerk.

Paul D. Irving, Sergeant at Arms, was sworn in as Sergeant at Arms of the House of Representatives on January 17, 2012. He is the 36th individual to serve as Sergeant at Arms, an office that goes back to the first Congress in 1789. He is the chief law enforcement and protocol officer of the House and is responsible for maintaining order on the House side of the United States Capitol complex.

Paul Kiko, who is the Chief Administrative Officer, was sworn in as Chief Administrative Officer of the House on August 1, 2016. He is the eighth person to serve as Chief Administrative Officer since the position was created in 1995. He is responsible for the information technology, financial, logistic, human resources, and procurement services provided to Members and their staff.

Michael Ptasienski was appointed as the fifth Inspector General of the House on February 15, 2018. Prior to being appointed IG,

he served in the IG's Office as the Deputy Inspector General, Advisory Administrative Services, and as the Director of Management Advisory Services.

It is my pleasure to welcome our witnesses to the Committee this morning.

Each of you will be recognized for 5 minutes, but your entire written statement will be made part of the record, so we encourage you to summarize it. As you know, we have a lighting system, and when you hit 1 minute, the yellow light will show up. When it turns red, your time is up and we would ask you to try to wrap up.

So, first, we will turn to you, Ms. Johnson, for your testimony. And welcome.

STATEMENTS OF THE HONORABLE CHERYL L. JOHNSON, CLERK OF THE U.S. HOUSE OF REPRESENTATIVES; THE HONORABLE PAUL D. IRVING, SERGEANT AT ARMS, U.S. HOUSE OF REPRESENTATIVES; THE HONORABLE PHILIP G. KIKO, CHIEF ADMINISTRATIVE OFFICER, U.S. HOUSE OF REPRESENTATIVES; AND THE HONORABLE MICHAEL T. PTASIENSKI, INSPECTOR GENERAL, U.S. HOUSE OF REPRESENTATIVES

STATEMENT OF THE HONORABLE CHERYL L. JOHNSON

Ms. JOHNSON. Good morning. Chairperson Lofgren, Ranking Member Davis, Members of the Committee, thank you for this opportunity to testify about the priorities of the Office of the Clerk, and thank you for your guidance and support.

The Clerk's Office is a nonpartisan organization integral to the legislative process. We provide the procedural assistance and support necessary for the orderly conduct of official business of the House, its Members, and committees.

I will use my time to outline our four key priorities for 2019 and beyond, starting with the Legislative Information Management System modernization and redevelopment project, also known as LIMS.

LIMS enables the House to conduct legislative business and enables the public to follow that business. It brings in bill information, floor activity, Member and committee information, and executive communications from the House and Senate and distributes that information to GPO, the Library of Congress, Members, committees, House officers, and the public.

However, LIMS was built more than 30 years ago and operates on an outdated programming language on a very old platform. The cost and technological risk of continuing on this platform are high, as finding skilled developers to work on legacy platforms is difficult and maintaining the current system demands significant resources.

Migrating LIMS to a modern technology will allow it to be more flexible to readily incorporate changes and accept new legislative requirements while maintaining a high level of security to better meet the House needs.

A second key priority is supporting committees.

As part of our efforts to improve communications and strengthen relationships with House staff, we collaborated with the Parliamen-

tarian and the CRS and Congressional Staff Academy to host a briefing in January for all committee clerks. The briefing provided new and veteran clerks with tools they need to do their jobs and included sessions on the legislative process. We plan to continue our training series throughout the year.

In addition, our Official Reporters provide reporting services for all Committee markups, hearings, and depositions as well as for investigative interviews. These services are subject to increased demand given the expanded deposition authority and oversight needs. In fact, in the 3 short months of the 116th Congress, our Official Reporters have supported more than 460 hearings and markups.

The Comparative Print, or Posey Print project is a third key priority. This technology allows us to create comparisons between current law and what the law would be with the bill's proposed changes. Today, the Rules Committee and the office of the House Legislative Counsel have access to the document comparison tool. Our goal for the end of phase three in August 2020 is to expand the application to a single comparison tool and to expand access to all House staff.

Our fourth key priority is personnel development. We continue to evaluate training opportunities for our staff to ensure they align with our mission and goals and to enhance cross-training as employees with specialized skills retire. This initiative gives current employees hands-on experience in highly specialized areas and promotes career growth within the organization.

Our aim is to keep exceptional employees motivated by strengthening their current skills and helping them acquire new ones. We have established a thorough training plan to further develop our workforce talent and broaden our institutional memory to be able to promote from within and to ensure personnel transitions do not disrupt our operations.

We also will continue to recruit highly qualified new employees from a diverse pool of applicants.

We look forward to continuing to carry out our many other important responsibilities, as outlined in my written testimony. Thank you for this opportunity, and I look forward to your questions.

[The statement of Ms. Johnson follows:]

CLERK | UNITED STATES HOUSE
of REPRESENTATIVES

....

STATEMENT BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION

"HOUSE OFFICER PRIORITIES FOR 2019 AND BEYOND"

THE HONORABLE CHERYL L. JOHNSON
APRIL 9, 2019

....

Chairperson Lofgren and Ranking Member Davis, Members of the Committee: Thank you for the opportunity to testify about the priorities and operations of the Office of the Clerk and for your guidance and support.

From the introduction of new bills on the House Floor to the delivery of enrolled bills to the White House for presentment to the President, our office is integral to the legislative process. The Clerk's Office is a nonpartisan organization that provides the procedural assistance and support necessary for the orderly conduct of official business of the House of Representatives, its Members, and Committees.

GOALS FOR THE 116TH CONGRESS

For the 116th Congress, the Office of the Clerk's goals include continuing to ensure the integrity and modernization of the legislative process and improve public access to House Floor and Committee proceedings; supporting the work of House Committees; and ensuring that we support our outstanding staff, and where necessary recruit new staff, in a way that our employees can continue to flourish in their jobs and fully support this institution.

KEY PRIORITIES FOR THE 116TH CONGRESS

Legislative Information Management System Modernization and Redevelopment

One key priority within our goals for the 116th Congress is the ongoing Legislative Information Management System (LIMS) modernization and redevelopment project. LIMS is a critical part of the flow of legislative information. It brings in bill information, Floor activity, Member and Committee information, and Executive Communications from the House and Senate and distributes that information to the Government Publishing Office (GPO), the Library of Congress, Members, Committees, House Officers, and the public.

However, the LIMS system was built more than 30 years ago and operates with an outdated programming language on a legacy platform from the mainframe era. The platform has undergone multiple migrations and currently runs in the Linux environment. However, the legacy codebase has not been upgraded and poses significant challenges moving forward. The cost and technological risk of continuing on this legacy platform are very high as finding skilled developers who can work on legacy platforms is difficult and maintenance and changes to the current system demand significant resources.

The migration of LIMS to a new modern technology will allow the application to be more flexible, extensible, robust and secure, and ultimately enable it to better meet the House's needs. This phase of the modernization project will comprise LIMS data modeling, backend

development, Floor Action Reporting System (FARS), Committee Action Reporting System (CARS), Executive Action Reporting System (EARS), Reports Due to Congress, Senate Action Reporting System (SARS), and Quality Assurance Testing.

Support for House Committees

Our second key priority is support for House Committees. That is why as part of the Office of the Clerk's ongoing efforts to improve communications and strengthen relationships with the House staff we serve, our staff collaborated with the Parliamentarian's Office, the Congressional Research Service, and the Congressional Staff Academy to host a briefing in January for majority and minority Committee clerks. The briefing provided new and veteran clerks with the tools and information they need to do their jobs in the 116th Congress and included sessions on the legislative process, administrative services and resources, and technical training. Session topics included

- Filing Committee reports
- Completing the new Truth in Testimony Form
- Submitting remarks for the *Congressional Record*
- Archiving Committee records
- Reporting Committee actions to appear on Congress.gov
- Updating the Committee Repository

We plan to continue our training offerings throughout the year.

In addition, the official reporters provide reporting services for all Committee markups, hearings, and depositions as well as for investigative interviews. These services remain subject to the potential for increased demand as a result of expanded deposition authority and oversight needs. In fact, so far this Congress, our Office of Official Reporters has supported more than 460 hearings and markups.

The Clerk's Office, following a directive in the Committee report accompanying our fiscal year 2019 appropriation, researched language for a standardized electronic Truth in Testimony Form. With the help of this Committee, our office held information sessions with other Committees' staff to solicit ideas and incorporate feedback. The Office finalized the form, received approval for its use in the 116th Congress, and made it available on HouseNet.

The Clerk's Office also develops and maintains the Committee Repository website at https://docs.house.gov. This online portal enables the public to track hearing and markup schedules, meeting notices, testimony, truth-in-testimony disclosures, opening statements, legislative text and amendments, and recorded votes. The House has made great progress in

increasing the transparency of Committee proceedings, and the Clerk's Office is proud to support that effort.

Comparative Print Project

The Comparative Print project is a third key priority. After the successful completion of Phase 1 of the Comparative Print project at the end of 2017, the Clerk's Office has continued to work with the Office of the Legislative Counsel and the Law Revision Counsel on the planning and development of subsequent phases.

In August 2018, the Clerk's Office awarded the contract for Phases 2 and 3 of the Comparative Print project. Phase 2 is anticipated to last from August 2018 to August 2019 with the following deliverables:

- Develop and build the backend framework to include security, user management, document repository, and document transformation—in progress, second quarter 2019
- Build natural language processor (NLP) to interpret amendatory language —initial design complete (fourth quarter 2018), in progress, first/second quarter 2019
- Implement base set of amendatory language and automated execution to create a stand-alone document that meets the provisions of clause 12(a) of House Rule XXI—second quarter 2019
- Implement an editor for those cases in which user intervention is needed—second/third quarter 2019
- Continuously improve the comparison document in HTML and PDF that meets the provisions of clause 12(b) of House Rule XXI—second/third quarter 2019
- Improve billcompare.house.gov user interface—second/third quarter 2019
- Develop outputs in HTML, PDF, and XML—second/third quarter 2019.

Phase 2 of the project is on track and we are holding weekly status meetings with the vendor. We expect Phase 3 of the project to begin later this year and anticipate it will last from August 2019 to August 2020. Below are the deliverables for Phase 3:

- Continue to build and refine NLP engine and implement an extended set of amendatory language—first/second quarter 2019
- Refine Phase 2 functionality: automation, editor, transformations, and user interface—third quarter 2020
- Migrate the current Amendment Impact Program (AIP) to the Posey Technology—fourth quarter 2019
- Deploy to larger user base—second quarter 2020
- Develop outputs in HTML, PDF, and XML—third quarter 2020.

Personnel Development

The fourth of our key priorities is personnel development. The Clerk's Office continues to evaluate training opportunities for our staff to ensure they align with our mission and goals and to enhance cross-training as employees with specialized skills retire. This initiative gives current employees hands-on experience in highly specialized areas and opens the door for career growth within the organization.

Our aim is to keep exceptional employees motivated by strengthening their current skills and helping them acquire new ones. We have established a thorough training plan to further develop our workforce talent and expand our institutional memory, to be able to promote from within, and to ensure personnel transitions do not disrupt our operations.

We have also begun to implement a cloud-based performance review system that will allow us to standardize evaluation criteria, goal-setting, and feedback across the Clerk's organization. We are currently testing the system and plan to provide user training during the second quarter of 2019.

Finally, we will continue to recruit highly qualified new employees and will reach out to a diverse pool of applicants. As we plan for the future, we want to fill four new positions essential to supporting legislative proceedings: three for Legislative Computer Systems, which are needed to meet increasing transparency, efficiency, LIMS, and cybersecurity project requests, and a fourth in the Office of House Employment Counsel (OHEC) to support compliance with recent amendments to the Congressional Accountability Act (CAA) and related workplace rights reform measures.

ADDITIONAL IMPORTANT ONGOING RESPONSIBILITIES AND POINTS OF EMPHASIS

We also look forward to continuing to carry out our many other important ongoing responsibilities and points of emphasis this Congress, which include the following:

Support for Legislative Proceedings

In recent years, the Clerk's Office has made significant improvements to *Reports to be Made to Congress*, a document required to be published at the beginning of each session of Congress. This document lists all of the reports that any officer or Department is required to make to Congress. Most recently, we collaborated with the Library of Congress to make the Executive Communications and Requirements data sets available on Congress.gov. This addition is a further enhancement to the interface and search capabilities of the system and follows earlier work to link reports received to their corresponding statutory requirements.

The Clerk's Office supports the legislative process from introduction to engrossment and presentment. The bill clerks process all bills and resolutions when they are introduced. The tally clerks record all Floor votes cast through the Electronic Voting System (EVS) and manually in the Well of the House, maintain the *House Calendar*, and process all Committee reports filed with the House. The journal clerks produce the constitutionally mandated *Journal of the House of Representatives* and handle all Presidential Messages.

When bills and resolutions pass the House, the enrolling clerks prepare the official text for transmission to the Senate or the White House. Along with their more visible duties of announcing pending business on the Floor, the reading clerks deliver bills and messages to the Senate. Our staff is hard at work, including whenever the House is in session—day or night—supporting the work of the House of Representatives.

In addition to supporting House Floor operations, the Clerk's Office is responsible for making the proceedings of the House easily accessible to the public and Members alike. The Clerk's Office hosts the publicly available website, *Bills to be Considered on the House Floor*, at https://docs.house.gov. This site is the central source for all legislation scheduled to be considered on the Floor each week.

Our staff maintains and updates the online summary of Floor proceedings, including information on pending legislation and votes taken, on our website at http://clerk.house.gov. The Clerk's Office also maintains live and archived video of all House Floor proceedings at http://HouseLive.gov and provides closed-captioning services to ensure that House proceedings are accessible to all. Our official reporters transcribe Floor debate from gavel to gavel. We provide these transcripts along with other legislative data to GPO, which makes them available the next day online and in print in the *Congressional Record*. The Clerk's Office also makes daily updates to the bill summary information at Congress.gov.

Electronic Voting System

The EVS has three main components: the EVS Server, vote stations, and the display subsystems, which include the summary displays (updated in 2009) and the main displays (updated in 2010). We completed the vote station upgrade in August 2018. We are planning to upgrade the Venus Display Servers (part of the display system) and replace all the work stations on the House Floor during the August 2019 District Work Period. We will continue to perform routine maintenance as needed.

We have also begun discussions with our vendor to develop a plan for ongoing support of the House Floor displays. When the summary displays (2009) and main displays (2010) were installed we anticipated a 100,000-hours or 10-year lifespan. We are not close to the 100,000 hours, but we are approaching the 10 years, so we want to plan for potential power supply and fan replacements.

Consensus Calendar

Section 102, Subsection (r), of H.Res. 6 provides for a Consensus Calendar in the 116th Congress House Rules and mandates that the Speaker must designate, and the House must consider, at least one measure on the Consensus Calendar during any week in which the House convenes (except before March 1 at the beginning of a Congress and after September 30 at the end of a Congress). This subsection also provides that to be eligible for placement on the Consensus Calendar a measure must accumulate 290 cosponsors and must not have been reported by its primary Committee of jurisdiction. When this cosponsorship threshold is reached the sponsor of the measure may, while the House is in session, submit to the Clerk a written motion to place the measure on the Consensus Calendar. If these conditions have been met, the Clerk will note the motion's submission in the *Congressional Record* of that day and enter the motion on a comprehensive list of Consensus Calendar Motions, which will be available on the Clerk's website. After a measure has maintained at least 290 cosponsors for a cumulative period of 25 legislative days after the presentation of the motion, the measure will be placed on the Consensus Calendar, where it will remain until it is considered in the House or reported by the primary Committee. The Clerk's Office has developed a process that will ensure it meets the Consensus Calendar requirements.

Support for the 116th Congress

On November 14, 2018, the Clerk, Deputy Clerk, and Senior Advisor to the Clerk welcomed Members-elect to the Capitol during New Member Orientation in the House Chamber. During the session, they provided an introduction to Office of the Clerk services, the EVS, and rostrum staff. On January 3, 2019, the Clerk led the Opening Day activities in the Chamber through the election of the new Speaker. In preparation for the new Congress, Clerk staff updated the EVS and all other systems as well as House Floor materials, including Roll Call books, *House Journal* files, and manual tally sheets. The Office also worked with Secretaries of State and other state election officials to review all Certificates of Election.

Support for Members

The Capitol Service Groups maintain the Lindy Claiborne Boggs Congressional Women's Reading Room, the Members and Family Committee Room, and the Congressional Prayer Room, which are near the House Chamber and provide spaces for rest and reflection.

The Clerk's Office worked with the Architect of the Capitol to design, produce, and install a permanent display of current women Member photographs in the Lindy Boggs Room. The Office also created a digital photographic display of all former women Members. These installations replaced 20 individual frames and several print posters, which hung in the

space for more than 15 years, and allow for quick updates in the future to accommodate the growing number of women Members.

The House Library provides research services for legislative staff of Members and Committees. The Library offers an online portal at https://library.house.gov/site with comprehensive guides to legislative research topics and regular training with our Congressional Staff Academy partners.

OHEC provides House employing offices with legal counsel and training on employment matters, including anti-discrimination/anti-harassment laws, family and medical leave, disabilities law, fair labor standards requirements, workplace safety, and other issues arising under the CAA and recent amendments to the statute and related reform measures.

Operation of Vacant Offices

Under the Rules of the House of Representatives, the Clerk becomes the employing and certifying authority when a vacancy occurs, and we work with the remaining staff to continue the Office's operations and provide constituent services until a successor is elected. The Clerk's Office has managed three vacant offices to date this Congress.

Website Redesign

The Clerk's Office will soon release the Beta version of our new redesigned website at https://clerkpreview.house.gov. The new homepage highlights House Floor activity and provides easy access to vital legislative information in a user-friendly, responsive, and modern design. We have added several features, including a public vote search page, updated Member and Committee profiles, and a new video streaming site (https://live.house.gov) that includes the ability to rewind the live feed and search closed-captioned text. The Clerk's Office also released an Alpha version of a new internal video clipping tool (http://floorclips.house.gov). The last major piece of the Clerk website redesign is a new site search tool, which is expected to be ready in June 2019.

Public Disclosure Services

By law and under the Rules of the House of Representatives, the Clerk's Office is charged with providing public disclosure information that helps preserve the integrity and increase the transparency of the legislative process. Our Legislative Resource Center manages the filing and retention of this information and responds to public inquiries regarding the legislative activities of the current Congress.

Financial Disclosure

The Clerk's Office administers the filing of and public access to all financial disclosure forms and periodic transaction reports submitted by House Members, Officers, candidates, and

senior House staff, as well as disclosures filed by employees of the Capitol Police, Library of Congress, GPO, Botanic Gardens, and the Congressional Budget Office. We maintain the online filing system for these reports and work closely with the Ethics Committee to continue to improve both the filing system and public access to the records on our website. We have seen a steady increase in electronic filings since the system was implemented—from 68 percent of filings in 2013 to 87 percent in 2018.

Lobbying Disclosure

The Clerk's Office continues to support the lobbying disclosure filing system in coordination with the Secretary of the Senate, who shares responsibility for administering the filing requirements of the Lobbying Disclosure Act (LDA). We make these filings available online in a searchable, sortable, and downloadable format. To assist filers, the Office also regularly reviews its Guidance to filers and updates it as warranted. The Guidance is available online at https://lobbyingdisclosure.house.gov.

Justice Against Corruption on K Street Act of 2018

The Clerk's Office is implementing the Justice Against Corruption on K Street Act of 2018 passed on December 20, 2018, and signed into law by the President. The "JACK" Act became effective on January 3, 2019, and amends the LDA by requiring all registrations (form LD-1) and quarterly reports (form LD-2) filed on or after January 3, 2019, to include

> "for any listed lobbyist who was convicted in a Federal or State court of an offense involving bribery, extortion, embezzlement, an illegal kickback, tax evasion, fraud, a conflict of interest, making a false statement, perjury, or money laundering, the date of the conviction and a description of the offense."

The Clerk and the Secretary of the Senate notified registrants in January that our offices were developing the technical changes necessary on the two relevant forms to meet this reporting requirement. We made those changes and posted additional guidance, on March 29, 2019, and notified filers that the updates are available in the system. If the statutory timelines required them to file a registration or quarterly report before the amended forms were available, we advised them to do so, and, if necessary, amend the filing to include the relevant information when it became possible to do so. Below are the project deliverables and estimated timeframes:

- February 8, 2019: Define additional fields, schema, and modified XML (complete)
- March 8, 2019: Complete updates to LD-1/LD-2 and data import modules and begin testing (complete)
- March 31, 2019: Complete updated forms and move to production (complete)
- May 2019: Complete new search/download site

Lobbying Disclosure Enhancements

We continue to consider an enhanced web-based lobbying disclosure system to improve submission of individual and bulk reports. We aim to improve the administrative functions of the system to ensure robust filing statistics and search capabilities and to enable direct approval of pending reports. By creating a unique lobbyist identifier, we will be able to synchronize House and Senate notification, approval, reporting, and referral efforts. The enhanced disclosure system is an item that remains on our priority list but has been pushed back because of the addition of unforeseen projects.

Franking

The Clerk's Office worked with the Franking Commission and the House Information Resources group from the Office of the Chief Administrative Officer to install a dedicated computer kiosk in the Legislative Resource Center to make franking filings available to the public electronically.

House Operations

Cannon Renovation and Relocation

Our office supports the ongoing renovation of the Cannon House Office Building, both directly and as a building occupant. The curatorial team provides staff and equipment to preserve, relocate, and store historical artwork located in construction areas. As the Cannon Renewal Project progressed from Phase 1 to Phase 2, the Office of the Clerk continued to move operations, personnel, and materials to new locations while maintaining continuity of services. In December 2018, the Legislative Resource Center's Public Information, Requisitions and Document Production, and Executive Communications subdivisions and several House Library staffers moved to their new office locations in the Cannon building. The House Library is now open in its new location.

Increased Storage for Congressional Records

The Center for Legislative Archives, part of the National Archives and Records Administration (NARA), maintains, preserves, and provides public access to archived House records pursuant to House Rules. In 2017 we secured storage space in two GPO buildings near the Capitol and obtained funding for the conversion of the first building, which we expect to occupy early in 2019. In 2018 we obtained funding for the conversion of the second building. With this additional space, the Center will have sufficient capacity to store House and Senate documents for decades to come.

High-Speed Printing

The Clerk's Office provides printed legislative materials for use on the House Floor and in Committee hearings, and for distribution to congressional staff and the public. In December we completed the purchase and installation of a new high-production black and white printer, which increases printing speeds by 22 percent over the previous printer and includes a booklet maker. The new printer ensures that the Legislative Resource Center can continue to quickly and reliably support legislative activities that require daily high-volume print jobs, such as House Committee hearings, bills, and reports. The Clerk's Office has also initiated a project to replace its older color printer this year to improve our production quality and speed.

Turner Redstone Data Center

The Clerk's Office postponed our initial plans to migrate to the new Turner Redstone Data Center in December 2018 because of changing legislative priorities and problems at the current Alternate Computing Facility backup site. We have rescheduled our migration for April 2019.

Archives, Art, and History of the House

The Office of Art and Archives within the Clerk's Office cares for the House Collection of fine art and artifacts, processes House and Committee records and oversees their eventual safe transfer to NARA, advises Members on their congressional papers, and provides informational services concerning the House's records, art, and history.

Archives

The Clerk's Office preserves the House's archived records. Our professional archivists help Committees to comply with their archival obligations and to research and retrieve records in their archives.

Since 2016 the Clerk's Office has showcased a searchable selection of official House records at https://history.house.gov/Collection/Search/. The Records Search collection illustrates the institution's work, its responses to issues of the day, and its relationship with the public and other branches of government. Highlighted records include documents from all 50 states as well as the District of Columbia and the territories, petitions and memorials, correspondence with Members, certificates of election, hearing transcripts, and maps and charts. We pair each record with a brief description that provides context and links to related material. Most recently, we added materials from all standing Committees as well as material from special and select Committees.

During 2018 the Clerk chaired two meetings of the Advisory Committee on the Records of Congress. The Office of Art and Archives and the Office of Communications worked with the

Senate and NARA to publish the *Sixth Report* of the Advisory Committee on the Records of Congress. The mandated report details many Committee efforts from January 2013 through December 2018, including new storage spaces for congressional records at GPO buildings; preservation of Committee hearing videos, social media, and Member office correspondence management systems data; progress on the project to refine descriptions of congressional records; and advances in digital curation.

Art and History

The curatorial staff of the Clerk's Office preserves the historical art and artifacts in the House collection and makes them accessible to the public. Our History, Art & Archives website at https://history.house.gov continues to enhance our ability to bring the history of the House to the American people even if they are unable to visit the Capitol. With sections on the Institution, People, Exhibitions and Publications, Collections, Oral History, Education, and Records and Research, the website offers a broad selection of material about the history and collections of the House and is a tremendous resource for the public and educators. In addition to its public outreach efforts and ongoing work with the permanent collections, the curatorial staff also manages several exhibitions throughout the House. We look forward to the opening of a significant new exhibition, with permanent displays of objects of interest to Members, staff, and constituents, in the Cannon basement rotunda, which is a major hub of the House campus. Development is underway on *The House at Work/Work in the House*, with images and artifacts—from 1800s Chamber desks to first-generation BlackBerrys—that tell the story of the work that has gone on here for more than 200 years.

The Office of Art and Archives and the Historian also participated in meetings and working groups with congressional partners to develop content for the upcoming redesign of exhibits in the Capitol Visitor Center's galleries. We anticipate our involvement in the redesign efforts to continue through 2020.

The Historian published a book and an e-book edition of *Asian and Pacific Islander Americans in Congress, 1900–2017,* which adds to the series of books about Congress that already included *Women in Congress, Black Americans in Congress,* and *Hispanic Americans in Congress.* The Office of the Historian collaborated with the Office of the Clerk to write, edit, and produce the 50-page booklet *The People's House: A Guide to Its History, Spaces, and Traditions.* The publication introduces readers to Opening Day ceremonies; Floor proceedings; Capitol rooms and House Office Buildings; art and artifacts in the House Chamber; and Leadership offices, political parties, and Officers. The Historian plans to make the content publically available on the History, Art & Archives website.

Biographical Directory of the U.S. Congress

We have continued to redevelop the *Biographical Directory of the U.S. Congress* (BioGuide) website (http://bioguide.congress.gov). Upgrades include a robust search engine, responsive user interfaces, and a content management system that will enable House and Senate Historians to enter more extensive profile data and collaborate seamlessly. The Clerk's Office expects to launch the Alpha version of the website during the first half of 2019.

Thank you again for your continued guidance and support and for the opportunity to testify.

The CHAIRPERSON. Thank you very much.

We will turn to you, Mr. Irving.

STATEMENT OF THE HONORABLE PAUL D. IRVING

Mr. IRVING. Good morning, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. I appreciate the opportunity to present the Office of the Sergeant at Arms operational priorities for 2019. It is an honor and a privilege to serve this institution, and I look forward to working with the Committee as the year progresses.

As noted, although I have submitted my full testimony for the record, I would like to briefly highlight and update the Committee on a number of security initiatives for 2019.

In the past few years, the Sergeant at Arms, in conjunction with the Capitol Police, has enhanced security services, to include screening prior to entry of our buildings, developed an enhanced security focus to assist Members in this increased threat environment, expanded security services into district offices and district-based events, and moved the Capitol complex closer to 100 percent screening by bringing the House office buildings into the secure perimeter.

Unfortunately, many Members receive threats and direction of interest communications that raise concerns for them, their families, and their staffs. In light of these threats and concerning communications, my office interfaces with Members' offices seeking security coordination for off-campus events in the Washington, D.C., area, in their districts, or elsewhere across the country.

We work with the Capitol Police to provide a level of protective support that is based on threat intelligence and proactive criteria which may form the basis of an enhanced level of support. Protective services can range from security awareness briefings in the Member's district to a request for local law enforcement support for a public appearance by the Member, and also deployment to the Member's district by the Capitol Police.

In regard to district office security, my office continues to build upon the success of our District Office Security Program that was launched in the summer of 2017. Since its inception, the program has assisted 390 district offices with the installation of intrusion-detection systems, alarms, cameras, panic buttons, and coordinated local law enforcement support of nearly 450 events and townhalls across the country. We have also documented nearly 13,000 outreach interactions with Members and their offices. In addition, my office has distributed 386 mail hoods to help protect district staff when opening mail.

Focusing on the Capitol complex, we are working toward the implementation of House garage security to ensure full screening into the House office buildings and in line with the Capitol and Senate office buildings. I am pleased to announce that, with the assistance of this Committee, security screening from all garages will be ready for implementation this year.

One of our largest operational initiatives is the Joint Audible Warning System. This is a shared effort with the Capitol Police, the Architect of the Capitol, and the Senate Sergeant at Arms to replace the aging emergency annunciator system introduced as a

temporary measure following the events of 9/11. The system components of these pager-like devices, located in all D.C. offices, are beyond their end-of-life dates, the technology is outdated, the battery components are no longer manufactured, and the system support from the vendor is limited. Seventeen years after implementation, we are seeking a new, separate, non-cell-tower-based system for emergency notifications throughout the House to ensure that emergency voice notifications are transmitted via secure radiofrequency to all offices and meeting rooms throughout the campus.

As I have noted, a more detailed listing of my operational priorities are provided in my extended testimony, such as replacement of the GSA-rated safes for Members to store classified and sensitive information.

Thank you again for the opportunity to appear before the Committee. I am so appreciative of the Committee's unyielding support and our partnership as we strive to maintain the delicate balance between strong security measures and a free and open campus to the Capitol complex.

I am happy to answer any questions you may have. Thank you.

[The statement of Mr. Irving follows:]

Office of the Sergeant at Arms
Operational Priorities

Statement of the Honorable Paul D. Irving
Sergeant at Arms
U.S. House of Representatives
Before
The Committee on House Administration

Good morning Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. I appreciate the opportunity to present the Office of the Sergeant at Arms' operational priorities. It is an honor and a privilege to serve this institution, and I look forward to continuing to partner with the Committee on these priorities as this year progresses.

Since 1789, the daily responsibilities and expectations of the Sergeant at Arms have changed significantly. Within the last few years, the Sergeant at Arms Office has reexamined the security needs of the institution and transformed its mission, response and character. Members of Congress now receive an unprecedented number of threats and threatening communications, which mandate a proactive approach to our security posture.

I would like to highlight and update the Committee on a few initiatives that are either in place or in a planned implementation phase.

The Sergeant at Arms, in conjunction with the Capitol Police, has enhanced security services to include screening prior to entry of our buildings, developed an enhanced security focus to assist Members in this increased threat environment, expanded security services into District offices and District–based events, and is moving the Capitol complex closer to 100% screening by bringing the House Office Buildings into the secure perimeter.

Screening of visitors outside our buildings is designed to identify and mitigate threats before they reach the interior of our buildings. Physical security planning for the Capitol complex starts with pre-screeners at the outer perimeter and moves inward. In response to global terrorist threats, we have significantly enhanced the K-9 teams and officer pre-screeners outside the building entrances. I am working with the Architect of the Capitol on a planned Capitol South Door Screening Kiosk to move visitor screening outside the Capitol and into an appropriately sized screening kiosk adjacent to the Capitol. Not only will this kiosk ensure that all visitors are

screened outside the Capitol building, it will also provide the thousands of visitors to the House Chamber an indoor waiting area that will greatly enhance their experience. The ongoing design phase is a collaboration with the Architect of the Capitol, the Sergeant at Arms office, and the Capitol Police.

Many Members receive threats and direction of interest communications that raise concerns for the Members, their families, and staff, but do not equate to the requirement of a Capitol Police protective detail. The number of threatening communications has increased three-fold over the past few years. In light of this increase, my office interfaces with Members' offices seeking security coordination for off-campus events in the Washington, DC area or elsewhere across the country. Upon receiving a request for law enforcement support, the Sergeant at Arms will request the Capitol Police conduct a security survey and/or risk assessment to determine what protective services are needed and if those services will be provided by Capitol Police and/or cooperating federal, state and local law enforcement partners. Furthermore, I have tasked my office to provide a level of protective support that is based on a proactive set of criteria which forms the basis of an enhanced level of support, such as an increased public profile on social media platforms. Protective services can range from a notification to local law enforcement, to additional assistance to the Member's District Office staff, to a Capitol Police deployment.

The Office of the Sergeant at Arms continues to build upon the success of our District Office Security Program that was launched in the summer of 2017. To assist in the facilitation of our District Office Security Program, I established the District Security Service Center. The District Security Service Center serves as a "one stop shop" for all district security matters. Since its inception, the program has assisted 390 district offices with the installation of intrusion detection security alarms, cameras and panic buttons. In addition, my office continues to pay for security upgrades at one district office per Member and pays for the alarm system monitoring fees for multiple offices. I would like to thank the Committee for its ongoing support of this vital security program.

Since the start of the 116th Congress transition, we have assisted each freshman Member in evaluating their security options for new district offices. 88 freshman Members have made a decision on security upgrades for at least one district office and, we are working with the remaining offices to assist them in evaluating their security options.

During New Member Orientation, the SAA and CAO, with support from the Committee, encouraged Member-elects to select their predecessor's space whenever possible. As a result, nearly one third of district office spaces acquired to date are spaces already containing a House installed security system. The District Security Service Center has assisted in the completion of approximately 50 new security assessments with an additional 10 to be completed in the coming days and weeks. Security upgrades have been completed at 15 district offices.

In conjunction with the CAO, the District Office Security Center coordinates and distributes mail hoods to district offices. The mail hoods allow a Member's district office to improve the safety and security of their office by providing a more secure method to open mail. In response to offices continuing to receive suspicious and/or threatening mail, we increased our allotment of mail hoods by 10% to support additional interest in the program and replace damaged/aging units. Increasing participation in our mail hood program has been a primary goal during this transition. Similar to the security systems, this program is opt-in meaning the Member district must inform us as to which office we should send the mail hood. Additionally, throughout the year, we conduct periodic outreach to Member offices to ensure that they are aware of the program and to provide reminders to practice safe mail handling procedures. To date, 386 mail hoods are in use with 26 of these hoods in freshman Member district offices.

Last year, the District Office Security Service Center, in conjunction with Office of the Sergeant at Arms Police Services staff, helped to coordinate local law enforcement support for nearly 450 public events and town halls across the country. Since its inception, the District Office Security Service Center has documented nearly 13,000 outreach interactions with Members and their offices. While many of these interactions are at the request of the Member, the District Office Security Service Center is also proactive in its outreach. For example, we performed outreach following an active shooter incident in Thousand Oaks, California; the synagogue shooting in Pittsburgh, Pennsylvania; the series of package bombs in and around Austin, Texas; and most recently, the active shooter incident in Aurora, Illinois. This outreach ensures all staff are accounted for, provides guidance on protective actions, and disseminates pertinent contact information should any security related questions or concerns arise. The District Office Security Service Center team also proactively reaches out to district offices to educate staff on security

related information that is available to them. For example, this past year we reached out to each Member office that had not previously utilized our program to coordinate law enforcement support for public events. We recently launched two online webinars, one for active shooter training and one for safe mail handling procedures.

My office also conducts security awareness briefings in conjunction with the Capitol Police for District Offices. We will conduct these briefings in the district and we attempt to coordinate these briefings to maximize the number of offices that can be covered. The topics covered include the security resources available to congressional offices, event security and law enforcement coordination, threats and concerning communications, suspicious activity and protests, and district office security considerations. We have conducted 21 of the briefings in the last year.

Focusing on the Capitol complex, our largest Capitol security initiative is the Garage Security Enhancement Project, which will bring the entire Capitol complex closer to 100% screening by bringing the House Office Buildings into the secure perimeter and in line with the Senate Office Buildings and the Capitol. The Office of the Sergeant at Arms continues to work with this Committee, the Architect of the Capitol and the Capitol Police to implement screening in the House garages, so that all personnel entering the House Office Buildings from within the garages will be screened as those entering the buildings from the street. This will ensure the same level of screening whether using the pedestrian entrances or the garages to all House (and Senate) Office Buildings and the Capitol. I am proud to say that we will complete this initiative and be ready for screening from the Rayburn and Cannon Garages in June of this year.

The addition of the garage screening will eventually allow Members and staff to move from the House Office Buildings to the Capitol without additional interior magnetometer screening in the Rayburn and Cannon tunnels. I will continue to work with the Capitol Police and the Architect of the Capitol to minimize the inconvenience and impact of this project on Members, staff, and others who work in the House Office Buildings.

I am very proud of the work that has gone into these initiatives and the services my team provides to the House community.

In addition to these important ongoing projects, I would like highlight other operational security projects that my office is undertaking.

I am presently undertaking a shared effort with the Senate Sergeant at Arms, Architect of the Capitol, and Capitol Police to replace the aging wireless emergency annunciator system. The existing wireless annunciator system was introduced as a temporary measure following the events of 9/11. The system components of these pager-like devices (located in all DC offices) are beyond their end-of-life dates, the technology is old, battery components are no longer produced, and system support by the vendor is limited. 17 years after implementation, I am working with our security partners to procure a new joint audible warning system (JAWS), with encrypted transmission capabilities, and new devices for all offices in the House. It is critical for us to replace the system components, including the 2,500(plus) devices currently in every office, every hearing room, meeting room, and work area in the House-side of the Capitol, Capitol Visitor Center, and all five House Office Buildings.

With the new JAWS system, emergency voice notifications will be sent via secure radio frequency to all offices and meeting spaces throughout the campus. This radio frequency system will not rely on cell towers or IP-based networks and will provide a separate and critical system that will work in parallel with the other systems in place, to provide critical life-safety information to everyone in the House. Importantly, the encryption capability will help ensure messages are sent from trusted, authorized officials to verified devices.

The JAWS effort, in conjunction with other existing notification capabilities – the Joint Emergency Mass Notification System (or House Alert currently available on desktops and cellphones) and the Public Address System (the loud speaker system in office hallways) – will provide notification resiliency. Collectively, they will use multiple delivery methods - including email systems, cell towers, network systems, and soon radio frequencies - to send emergency messages to Members and staff.

Another important initiative for our office is the Safe Program. In 2017, the Committee shifted the management of GSA-approved safes from the Office of the Chief Administrative Officer to the Office of the Sergeant at Arms. This program includes the secure management, storage, training, and record keeping for close to 300 GSA-approved safes used in Member and

Committee offices in the House. Our office has inventoried and created a secure database to track and monitor the GSA-approved safes currently in use. Over half of these safes still utilize an analog combination lock, which has proven to be difficult to open and unreliable over time. For FY20, I have requested funding to purchase new safes, with digital combination locks that adhere to the U.S. Government's highest security standard, to protect classified and sensitive information in Member and Committee offices in the House Office Buildings.

Employees of the Sergeant at Arms Office are our strongest assets. I would like to thank the Committee for helping to establish positions throughout the Office of the Sergeant at Arms so that we can increase the level of service we provide to Members.

Thank you once again for the opportunity to appear before the Committee. I am so appreciative for the Committee's unyielding support and partnership as we strive to maintain the delicate balance between strong security measures and free and open access to the Capitol complex. I am happy to answer any questions you may have.

The CHAIRPERSON. Thank you very, very much.

Mr. Kiko.

STATEMENT OF THE HONORABLE PHILIP G. KIKO

Mr. KIKO. Good morning. I want to thank each of you for the opportunity to present the CAO's priorities, which include improving and expanding upon our customer services, advancing the House's cybersecurity posture and technology support, and modernizing its internal and customer-facing processes.

The CAO is the largest House-specific support organization, with over 700 employees who provide a broad spectrum of services. Our employees assist offices with voucher processing, logistics and asset management, technology support, payroll, wellness, child care, et cetera.

The CAO has taken on new responsibilities, such as facilitating the workplace rights training for an estimated 16,000 individuals last year and standing up the new Office of Employee Advocacy and assisting with various analyses of House practices and functions.

The services provided by the CAO, old and new, are critical to the House operations and must constantly evolve and improve to meet the needs of Members.

I recognize that major improvements need to be made with our financial and asset management services. We have been working hard on these. We have brought in outside consultants, we have been working with the Committee, and I believe there is light at the end of the tunnel.

But it is not just these major areas that we must work on improving. We must continuously improve all our services, make the customer experience better by putting them first, meet their needs, and seek ways to improve our services.

The CAO's mission at its 1995 inception was "to constantly and consistently listen to our customers, meet their needs, and seek ways to improve our services." The customers are Members. It is simple. The CAO is to listen, deliver, and improve.

And that is exactly what the organization's strategic plan put into motion: a process to better listen to our customers, deliver the services that they need, and to constantly improve.

It is changing the way we approach service delivery. We launched a new business unit. We rolled out professional development training for House staff and did training, as was mentioned, for clerks, House financial systems, et cetera.

We are enhancing House-wide services that save Members money, working to expand our technology services and reduce reliance on vendor support. Last Congress, our mailing services team corrected nearly 60 million mailing records for Members' offices, saving them $17 million in postage and $18 million in production services.

We have responded to the overwhelming demand for food service improvements.

And the CAO also has paramount responsibility, as we all know, in protecting the House against malicious actors constantly seeking to gain access to House data. In just 1 month, every month, the CAO blocks an estimated 1.6 billion unauthorized scan probes and

connections, including 300 million to 500 million cyber attacks and an average of 12.6 million questionable emails to thwart fishing attacks. In 2018, our cybersecurity office deployed 615,000 patches and 3,000 malicious indicators to over 16,000 network-connected devices on campus.

I am paying close attention to the issues raised before the Select Committee on the Modernization of Congress to ensure the CAO's priorities align with and meet the needs expressed by Members, including those related to constituent communications, the adoption of new technologies, compensation trends, and district office support.

Technology modernization is one area that the CAO is moving aggressively towards. Our fiscal year 2020 budget requests funding for a more aggressive cloud strategy and with the Committee's support, we will be moving into a cloud-first strategy for all new technology endeavors.

And while the House does allow the use of cloud tools and authorized several dozen for use, integrating these tools in the past has been too difficult. I would like to speed this process along. To help solve this problem, the CAO is considering creating a technology innovation lab where Members can test, evaluate, and share innovative technology and ideas.

I want to again thank you for presenting the CAO's priorities. I just want to close out by saying, since I have been at CAO, the process I am trying to do is Member-first, the processes that Members want, not necessarily what people in the CAO think is best.

Thank you.

[The statement of Mr. Kiko follows:]

Statement of
The Honorable Philip G. Kiko
Chief Administrative Officer
United States House of Representatives
Before the
The Committee on House Administration

April 2019

Summary Statement
Philip G. Kiko
Chief Administrative Officer

Chairperson Lofgren, Ranking Member Davis, and members of the Committee, thank you for the opportunity to present the Chief Administrative Officer's (CAO) priorities.

In its 2018 written update to the Committee, the CAO highlighted cybersecurity and operationalizing the organization's Strategic Plan as its top priorities. It also highlighted other major projects and service initiatives such as enhancing House-wide technology services, implementing new standards for IT and financial shared employees, deploying Workplace Rights and Responsibilities Education, and establishing the new Office of Employee Advocacy.

The CAO has advanced every initiative identified as a priority last year and has taken on new responsibilities such as overseeing the execution and delivery of a compensation study. Operationalizing its Strategic Plan has been the most impactful initiative, prompting across-the-board service improvements.

In 2017, when the CAO developed its Strategic Plan, it set out to place the organization on a path to better fulfill its original pledge to provide the House with forward-thinking, cutting-edge solutions. In its original mission statement, the CAO pledged to, "constantly and consistently listen to our customers, meet their needs, and seek ways to continuously improve our services to them." Similarly, the goals of the organization's Strategic Plan are to improve the CAO's customer services through greater solicitation and consideration of customer feedback and the House environment and to modernize its services.

Since its implementation, the Strategic Plan has reached nearly every CAO employee and has impacted the organization's broad spectrum of services – old and new. It even led to the creation of two new business units expressly dedicated to delivering exceptional customer service and prioritizing the use of the organization's finite resources.

With a focus on customer service and innovation per its Strategic Plan, the CAO has identified its priorities for this year and beyond. The organization is also paying close attention to the issues raised before the Select Committee on the Modernization of Congress to ensure its priorities align with and address the needs of Members. From evolving constituent communication technologies, to modernizing compensation and diversity practices, to enhancing district office support, the CAO understands its role and has set its priorities accordingly. In fact, the CAO is creating a technology innovation lab where Member offices will be able to test, evaluate, and share innovative tools and ideas.

The strategic priorities outlined in this testimony include improving and expanding upon the CAO's customer services, advancing the House's cybersecurity posture and technology support, and modernizing its internal and customer-facing processes.

The CAO's nearly 700 employees fulfill the organization's mission to serve Members and their staff – here in the nation's capital and across the country – by providing administrative, technical, and operational solutions so that they can perform their constitutional duties. We offer a diverse array of services delivered by a diverse, talented pool of employees.

As we continue to operationalize the Strategic Plan, we realize our vision to be an essential resource for every Member of the People's House through outstanding customer service delivered by exceptional employees. Significant progress has been made in the way we do business, but more can and will be done. It is my hope that the service improvements are apparent to the Members and their staff.

Again, thank you for the opportunity to present the CAO's priorities and for the Committee's continued support.

Strategic Plan

Initiated in the fall of 2016, the CAO's Strategic Plan was developed by a cross-functional, bottoms-up strategy team This strategy team defined the CAO's mission and laid out specific service-oriented objectives for goals that focused on **customers, process, stewardship,** and **employees**.

After the Plan was finalized in early 2017, the CAO quickly moved to operationalize it. The organization brought together an array of service providers who gathered feedback from the House community, closely examined service delivery models, and identified ways to improve and modernize its services.

Over the past two years, the implementation of the Plan has prompted significant changes to the CAO's business model and, in turn, what the CAO hopes are recognizable improvements to the services it provides.

Customers

The CAO has set out to understand how the House community interacts with our services and to improve our customers' experiences.

Implementing objectives under the Strategic Plan's customer goal led to the creation of an entirely new business unit dedicated to delivering exceptional customer service – the Customer Experience Center (CEC). The CEC is comprised of existing, revamped, and new capabilities focused on services provided to Members and their staff. It now includes streamlined creation and delivery of digital media, graphic art, and videography products under its House Creative Services division. Its new Congressional Staff Academy is delivering a professional development curriculum requested by House

offices. And its new, expanded Customer Advocate program is helping offices navigate and acquire the services they need in their Washington, D.C., and district offices.

To achieve its customer objectives, the CAO adopted practices common within the private sector to measure customer satisfaction by deploying point-of-service surveys. The surveys replace a hodgepodge of surveys previously and inconsistently deployed by the organization. The new survey tool, launched in March of 2017, initially covered six transactional services provided by CAO employees. Today, it surveys recipients of 33 services and has gathered 12,101 survey responses. The responses indicate an average rate of satisfaction with CAO services of over 96 percent.

Survey feedback – good and bad – has prompted process improvements in CAO service delivery. Escalation processes are now in place to respond to any actionable feedback, and supervisors are assigned to resolve any challenges in service delivery. The CAO is currently implementing a new in-house survey tool that will expand its survey capabilities to include more transactional services and consultative services.

Process
A primary process goal for the CAO is to modernize its services and increase the use of its services through greater consistency and accuracy.

In August 2018, the revamped Communications and Marketing division within the CEC condensed a list of 150 services provided by the CAO as identified by CAO employees, to a simplified working list of 31 primary services better understood by the CAO's customers: Member, Leadership, and Committee offices. This working list of primary services helps CAO employees understand and communicate the full scope of CAO offerings as seen through their customers' eyes.

To improve how we communicate and market our primary services, the Communications and Marketing team also launched new CAO-wide branding standards to ensure all new or modified services are properly branded and easily accessible. For example, services should consistently be referred to by the name customers associate them with and be accessible through known access points like HouseNet, MyServiceRequests, First Call, or the Technology Service Desk.

As part of an analysis of its internal operations, the CAO found that greater collaboration between its service providers is required to improve efficiency and reduce duplicative efforts and their associated costs. To facilitate greater collaboration, the CAO initiated its Cross-Functional Collaboration Program in the summer of 2018. The Program brings together every service division involved in each of a customer's primary CAO services to examine each step taken to fulfill that service. With that information, the Program then identifies opportunities to expedite service fulfillment and eliminate customer pain points. For example, the Cross-Functional Collaboration Program closely examined the CAO's fulfillment of special event service requests submitted to its First Call customer service center. The examination discovered that for any given event, approximately 14 teams execute 50 activities with 34 decision points using 4 House systems and 6 forms.

The examination identified 12 customer pain points and 14 ideas to improve and streamline the process.

The Program is on track to convene the corresponding business units to examine at least half of the CAO's primary services by the end of 2019.

In 2018, the CAO also established an organization-wide governance framework that promotes transparent and informed decision making and has resulted in greater collaboration between business units from the inception of a new or modified service.

Stewardship
The CAO's stewardship goal is to safeguard and optimize the use of House resources.

To fulfill its stewardship objectives, the CAO continues to implement the actionable recommendations provided by an independent firm in September 2017 following its comprehensive review of the CAO's financial services. The recommendations included that actions be taken to improve overall accuracy, accountability, and customer engagement services. Implementing the recommendations has prompted new, expanded leadership within the CAO's Office of Finance; a restructuring of the Office of Financial Counseling; a reorganization of the Office of Budget, Planning, and Analysis; and the development of financial policies and procedures that codify best practices, legal requirements, and industry standards to be upheld by all Finance staff.

Though progress has been made, the CAO fully acknowledges that there is still much work to be done to improve the consistency, accuracy, and reliability of its financial services.

Operationalizing the process objectives in its Strategic Plan also required the CAO to prioritize the use of its finite resources based on risks posed to the House and spurred the creation of its new Office of Risk Management. The new business unit absorbed the CAO's Internal Control and Audit Liaison and Remediation Programs. It also provided for the development and implementation of Enterprise Risk Management and Compliance Programs. The implementation of Enterprise Risk Management will provide management with risk-based data to inform decisions and provide the capability to target resources to the areas of highest risk, ensuring the CAO's mission and objectives are met.

Employees
CAO employees are more than just a commodity for the House. They play an integral role to House operations and are part of the House community. They are comprised of individuals with diverse skillsets, including cybersecurity engineers, accountants, and tradespeople. Similar to employees in Member, Leadership, and Committee offices, they require investments in their development.

Since the implementation of its Strategic Plan, major strides have been taken to improve the organization's talent framework, its performance and feedback processes, and its workforce optimization efforts.

In 2018, the organization implemented a new talent framework that includes improvements to its recruiting and hiring processes. These include increased consultative discussions with hiring managers to ensure recruitment strategies are tailored to meet their specific needs. In 2018, the CAO also started a two-year effort to design and deploy a set of strategic human capital activities. Currently underway, these efforts include the development of new competency models, updated position descriptions, new candidate assessment tools, and the deployment of career development and mentor programs. Each of these initiatives will benefit current and future CAO employees by providing a more clearly defined roadmap for their career.

The CAO is making an investment in the development of its employees in a number of ways. For example, the CAO launched a manager training series called *Empower Hour* and an organizational communication series for non-managerial CAO staff. These series were attended by hundreds of employees during the 115th Congress.

Another important employee initiative is the CAO Speaker Series. The Series was created during the 115th Congress to provide an opportunity for CAO staff to come together and hear from a variety of Members, House staff, and other prominent individuals on topics ranging from professional development to the institutional development of the House of Representatives. The CAO launched the Series to create more engagement and collaboration among CAO staff and the institution they serve and to give staff the opportunity to share ideas and foster discussion around new and innovative ideas for the organization.

To accomplish its performance objective, in 2018, the CAO fully deployed its new employee performance management program that includes mid-year and new hire evaluations. The revamped evaluations are customized to each employee's individual performance goals and gauge the employee's performance as it relates to the CAO's organizational goals established in the Strategic Plan.

These noted talent framework and performance accomplishments align with and support the CAO's workforce optimization objectives.

The CAO is also making progress on its workforce planning activities. Starting in early 2019, the CAO began to identify the criticality of vacancies across the organization by taking a structured and risk-based approach. The organization's workforce optimization activities will focus more specifically on the knowledge, skills, and abilities needed to successfully achieve its mission.

Expanded Customer Services

Central to the CAO's Strategic Plan is the organization's vision to deliver outstanding customer experiences. Through the implementation of its Strategic Plan, the CAO has

36

expanded and improved its existing services and their delivery models and expanded its catalogue of services provided to the House community. Specifically, it has sought to provide new services that help Members and their staff effectively perform their jobs in an environment that promotes greater work-life balance and overall wellness.

Customer Advocates
Since its launch in September 2017, the CAO's Customer Advocate program has expanded from two Advocates serving approximately 100 Member offices to five Advocates serving all 441 Member, Delegate, and Resident Commissioner offices. Working hand-in-hand with First Call, the Customer Advocates connect their assigned House offices with the CAO's technical, administrative, and operational experts and help facilitate and triage CAO services on their behalf. Since its inception, the Advocate program has been well received. They have helped offices navigate the CAO's broad spectrum of services and were especially instrumental in facilitating the transition process for freshman offices during the transition to the 116th Congress, participating in 95 Member-elect briefings.

Customer Advocates have also traveled to Members' district offices to ensure that they are aware of the CAO services available to them and to gather feedback on how the CAO can better meet their needs. Since the program started, Customer Advocates have visited district office staff from 42 congressional offices as of April 5, 2019. 20 additional offices will be visited by the end of May. District offices visited by Customer Advocates are located in California, Illinois, Maryland, Pennsylvania, Texas, Virginia and West Virginia. Of the 62 offices, 31 are freshman offices of the 116th Congress. Visits to freshman offices are focused on district office setup and the availability of CAO services. Going forward, the Advocates will visit district offices in their assigned regions on a reoccurring basis.

House Creative Services
To streamline and modernize its popular photography and graphic services, the CAO merged the two previously separate divisions and added videography capabilities to create House Creative Services – a one-stop shop for Member office digital and creative service needs. In July 2018, House Creative Services began beta testing a new House Creative Services online platform that enables offices to access, manage, and edit their photos and graphic designs and order prints online. The platform is now fully operational and supporting approximately 180 House offices. It will be aggressively marketed to the entire House later this year once the additional personnel necessary to support higher usage are onboarded.

During the 115th Congress, House Creative Services received and processed nearly 22,000 work orders. It also expanded its catalogue of services to include new products such as motion graphics and canvas prints.

Congressional Staff Academy
The new Congressional Staff Academy is delivering a professional development curriculum specifically requested by Member, Leadership, and Committee offices to

help employees best perform their job responsibilities. Unlike the former learning center, which didn't focus enough on professional development offerings for congressional staff, the Academy includes courses that help staff perform their duties, such as courses on appropriations law, official committee clerk procedures, House financial systems, and leadership training. For example, to support the mandatory House-wide transition to electronic voucher submissions in October 2018, the Academy launched new financial systems training courses with subject matter expert instructors and an on-demand, online course. Within two months, the Academy trained over 200 House employees on the new voucher submission requirements.

In February 2019, the Academy launched a new leadership series available in person or via live webcast that has been well received by Chiefs of Staff, District Directors, and senior staff. Using feedback collected through surveys, focus groups, and one-on-one interviews, the Academy is currently creating courses specifically requested by House offices focused on congressional communications, legislative processes, and D.C. and district office administration.

The Academy is also preparing to roll out House-wide access to LinkedIn Learning, an industry-leading learning resource with thousands of on-demand courses covering a broad spectrum of technical and developmental skillsets.

The Academy is improving the registration experience for employee training with the implementation of a cloud-based learning management system. Once fully operational, the platform will replace the existing three platforms in use and create a one-stop shop where employees can register for in-person courses, take online courses, and track their course completion status.

Food Services
To make sure Members, staff, and visitors have a variety of quality food options on campus, the CAO has taken a multipronged approach to food service delivery, which includes gathering community feedback, increasing branded food options, and implementing quality control oversight.

In January 2018, the CAO surveyed the House community on food services. The survey received an impressive 2,431 responses that indicated a strong desire for both cafeteria and branded food options. To that end, the CAO has worked to bring more branded options to the House such as D.C.-based &pizza, which opened in the Rayburn House Office Building in February, and Au Bon Pain, which opened in the Cannon House Office Building April 3. Two additional branded sites will also open on campus the Tuesday after Labor Day, including a Steak 'n Shake in Rayburn. These branded options are in addition to the popular Dunkin' Donuts, Baskin Robbins, and Subway options on campus and new pop-ups like Mission BBQ, Cosi, Dyvine BBQ in Motion, BIBIBOP, honeygrow, and others.

Since opening, these branded options have been well received. In fact, &pizza sold nearly 8,000 pizzas in its first month.

38

To ensure quality food offerings are provided in cafeterias by the House food vendor, the CAO conducts vigorous oversight and contract enforcement. This includes inspections and surveillance, tracking vendor performance, and regular meetings with the vendor's management team.

Considering that Members and staff often work long hours and rely on the on-campus food options, the CAO understands the importance of delivering a quality array of food options and will continue to make food services a priority.

Member Constituent Communications & Mailing Services

Whether it's social media, phone calls, email, letters, or townhalls, Members employ all means possible to communicate with their constituents and keep them informed. These efforts demand significant time and resources. In turn, constituents are increasingly employing the same methods to contact their representatives about pressing issues. In fact, the volume of inbound constituent communications has increased substantially over the past two years, making it difficult for offices to receive, process, and respond to communications in a timely fashion.

Facilitating Member-to-constituent and constituent-to-Member communications is one of the CAO's primary services that has been and remains one of its top priorities.

To advance technical engagement capabilities available for House offices, the CAO launched an analysis of constituent engagement platforms used by House offices, including Correspondence Management Systems (CMS). More specifically, a leading independent technology consultant has been engaged to conduct a three-phased assessment to identify the current challenges around constituent engagement, conduct market research for technology solutions to address those challenges, and develop a modernization roadmap that will serve as a playbook for attaining improved engagement platforms.

The assessment, which included direct feedback from Member offices facilitated by Customer Advocates, will evaluate the feasibility of expanding the use of more modern engagement capabilities such as live chat and chatbots, process automation, machine learning and artificial intelligence, and constituent satisfaction analysis. The assessment is in process and is expected to be completed by mid-2019.

The CAO is also working with existing CMS providers to integrate their correspondence platforms with the House's telecommunications and voicemail systems, reducing an office's need to manually enter caller data into CMS platforms.

To improve its constituent mailing services, the CAO consolidated all House mail-related operations under the CEC that were previously under three separate CAO divisions – Logistics & Support, Finance, and Acquisitions. These include postal address reconciliation services, D.C. and district office billing, and mail vendor contract management. Consolidating these operations and moving them under the CEC has

yielded process improvements and more direct office feedback. For example, in February 2018, the CAO's Mailing Services team worked with the U.S. Postal Service (USPS) to introduce the use of its Informed Delivery Program – a service that delivers daily email previews of constituents' USPS mail. It also established a House-wide account for its Informed Visibility Program in March 2018, allowing offices to enhance constituents' daily email previews with weblinks to their official House.gov sites and/or social media sites.

To expedite compliance with the monthly district office outbound mail reporting requirements, the CAO developed an online reporting system that launched in October 2018 and improves the reporting process for offices.

During the 115th Congress, the CAO's Mailing Services team reviewed nearly 250 million addresses for House offices and made corrections to nearly 60 million records, saving offices over $17 million in postage and $18 million in production costs. It has over 380 offices participating in the digital mail program and oversees the House mail screening processes that intake an estimated 12 million pieces of mail and 2 million packages annually. It successfully intercepted the first of multiple potentially lethal pipe bombs sent to elected officials in October 2018.

Employee Wellness Program
To empower House staff with the resources they need to cope with the demanding pace of life and work on Capitol Hill, the CAO launched a comprehensive House-wide wellness program. The first step entailed identifying an experienced program manager to convene and lead an advisory committee comprised of Legislative Branch professionals with knowledge of the House's unique environment and needs.

The program officially kicked off October 2018 with the launch of wellnesscenter.house.gov, a website designed to keep House staff informed of wellness topics and services ranging from mindfulness, nutrition, fitness, general health, and stress management.

The program is expected to expand its services in 2019 with a dedicated storefront and satellite locations in each House office building, newsletters, in-person and online courses for D.C. and district staff, and individual and group consultative services. As part of the wellness program, the CAO recently acquired a contract with LifeCare, a company providing work-life services for House staff. LifeCare provides personal guidance and support to assist House staff through major life events and common, stress-inducing challenges such as finding child care options, matching elderly parents with housing options, and assisting in college and financial aid planning. Additional platforms that deliver wellness coaching and health assessments will also be rolled out in 2019 along with special health and wellbeing events.

Employee Advocacy
To fulfill the House's desire that employees have access to legal counsel and representation in matters covered by the Congressional Accountability Act, the CAO

established the Office of Employee Advocacy in compliance with H. Res. 724, passed by the House in February 2018. By September 2018, the CAO had retained a well-credentialed employment and labor law attorney to serve as the Director of the Office of Employee Advocacy and, soon after, retained highly competent, experienced employment and litigation attorneys. By the end of this month, Employee Advocacy will be comprised of four attorneys (the Director, one Senior Associate Counsel, and two Associate Counsel) and a Paralegal. The office plans to hire a Legal Secretary in late spring 2019.

Working with the CAO's Communications and Marketing Team, Employee Advocacy has engaged a targeted marketing strategy to inform the House community of the office's mission and its no-charge, complainant-side legal services. The marketing initiative has included various forms of communications and outreach aimed at employees located in Washington, D.C., and in district offices across the country. The office has also established relationships with key House offices to facilitate the accommodation of its role in personnel and employee rights processes and has provided valuable input on existing training curriculum, including the Workplace Rights and Responsibilities Education.

Another essential step in Employee Advocacy's rollout has been the establishment of security policies and protocols. Within the CAO, Employee Advocacy has worked with House Information Resources to create a system that protects employees' electronic communications with Employee Advocacy and the office's files from detection or disclosure to individuals or entities without the authorization of Employee Advocacy.

Since opening its doors, Employee Advocacy has had the privilege of counseling and representing House employees on a wide range of matters. It has handled 74 legal issues and cases that House employees have presented to Employee Advocacy for consultation, advice, or representation. To date, matters addressed by the office's attorneys have included claims of harassment and hostile work environment; discrimination based on race, color, disability, and sex (including gender, parental status and pregnancy); retaliation based on protected activity; violations of the Family Medical Leave Act; and failure to accommodate health conditions. Employee Advocacy's workload continues to grow as awareness of the office grows and legislative changes alter the legal landscape (e.g., new Member liability provisions in the Congressional Accountability Act).

House of Representatives Child Care Center
Since its creation in 1987, the House Child Care Center, operated by the CAO, has provided child care services for House employees. While House child care demands have increased over the years, the capacity of the House's Child Care Center has not. To accommodate more House families, the CAO worked with the Architect of the Capitol and other Legislative Branch stakeholders to expand the Center's capacity and relocate a portion of its operations to the O'Neill House Office Building.

In January 2019, the Center's capacity more than doubled to 160 children, and all waitlisted preschoolers and House toddlers on the original waitlist were offered slots. Wait times for parents of children of all ages seeking admission were also significantly reduced. Once all O'Neill construction and expansion operations are completed and the Center has moved all of its operations to O'Neill, the Center will triple in size for a total capacity of 232 children. The expansion has provided the Center with an opportunity to build upon its success as a program accredited by the National Association for the Education of Young Children. Specifically, the expansion has prompted operational changes at the Center, including changes in administrative and faculty structure, classroom structure, the effective implementation of age-specific curriculum, oversight of the Center's health and sanitization policies, and admissions policies and procedures.

Workplace Rights and Responsibilities
To help Members and staff comply with the Workplace Rights and Responsibilities training requirements prescribed in H. Res. 630, the CAO worked expeditiously with the Committee to procure a vendor with the capability and expertise to develop and implement custom, in-person education courses for the entire House community based in Washington, D.C., and across the nation. Between January and March of 2018, the CAO solicited and vetted vendors from across the country and was ready to deploy custom training in April. The custom 90-minute education courses began on April 30, 2018, and included more than 400 live training sessions in Washington, D.C., and over 200 sessions in locations across the United States. By the end of the Second Session of the 115th Congress, the CAO delivered live training to approximately 16,000 individuals.

Working with the Committee, the CAO is examining options to improve the program's curriculum and/or delivery prior to its deployment during the First Session of the 116th Congress.

Compensation and Diversity Studies
The FY19 Legislative Branch Appropriations report requires the CAO to compile a House compensation study that includes a comparative analysis of the salaries and benefits of House, Executive Branch, and private sector employees. The study is also to identify compensation disparities that may exist between individuals from different ethnic and racial groups and working under different employing authorities with similar job responsibilities.

Similarly, the House Rules package for the 116th Congress requires the Office of Diversity and Inclusion to compile an annual diversity report that evaluates diversity in House employing offices. To prevent duplicative efforts and save money, the CAO developed and is deploying a statement of work to identify a contractor capable of compiling data necessary to satisfy the requirements of both mandates.

Cybersecurity, Technology Support, and Modernization

42

Securing the House network, providing technology support, and constantly seeking opportunities to innovate and modernize operations are critical initiatives to the CAO's strategic mission to deliver outstanding customer experiences.

Cybersecurity

Malicious actors use multiple evolving forms of cyberattacks in attempts to gain access to the House network. In just one month, the CAO blocks an estimated 1.6 billion unauthorized scans, probes, and connections aimed at the House and an average of 12.6 million questionable emails to thwart phishing attacks from reaching intended targets. In 2018, it deployed nearly 615,000 patches and 3,000 malicious indicators to over 16,000 network-connected devices across the country to counter known cybersecurity threats.

The House is undoubtedly a target of private and state-sponsored criminal cyber activity and maintaining a strong cyber defense program is a paramount responsibility for the CAO.

In 2018, the CAO maintained a strong cybersecurity posture through system compliance monitoring, enhanced Dark Web threat intelligence monitoring capabilities, and improved mobile platform security for smartphones and tablets connected to the House network. The Office of Cybersecurity also continues to share threat intelligence with other Legislative Branch agencies, Executive Branch agencies, and our international allies.

To improve cybersecurity awareness and maintain vigilance among all House network users, the CAO continues to conduct its annual system penetration testing and a quarterly phishing campaign in addition to the required annual cybersecurity awareness training.

In August 2018, the CAO deployed a new cloud firewall to better protect and secure House websites hosted at our cloud service provider. The new firewall provides an additional layer of security between cybercriminals and House websites hosted in the cloud. The CAO is also deploying enhanced cloud security capabilities that will identify unauthorized or rogue cloud services connected to the House network and assist the CAO in its review of cloud services for use by the House community.

To enhance secure access to House data via smartphones and tablets, HIR deployed a new identity management service software. The software uses multifactor authentication and allows users to access their files through mobile single sign-on security features with biometric sign-on capabilities. The new software was successfully rolled out to CAO employees and select users in November 2018 and provides them remote mobile access to their files from Box and OneDrive cloud storage applications. House-wide deployment of the new mobile access software is slated for mid-2019. Once fully deployed to network-connected mobile devices, the software and its multifactor authentication capabilities will be deployed to network-connected desktops,

which will ultimately eliminate the requirement for entering passwords during network login.

With the continued support of this Committee, the CAO will continue to enhance its cyber defense capabilities to match evolving threats.

Controls Over Privileged Access to the House Network & House Information Security Policies
Enhanced cyber defense technologies are vital to safeguarding the House network. However, these efforts must be reinforced by strong controls over access to the network and House Information Security Policies.

To strengthen controls over network access, the Committee directed the CAO to develop standards intended to protect the financial and IT integrity of the House. The standards – developed in late 2018 and implemented in January 2019 – include new controls over privileged access to the House network as well as access controls over House financial systems. They also limit the number of individuals with privileged access to the House network, require individuals to undergo background checks prior to being granted privileged access, and centralize the authorization processes within the CAO.

To date, the CAO has initiated the new vetting and access processes with 90 percent of House shared administrative employees and is working with the remaining shared employees to fully implement the standards. Considering that these procedures are new, the CAO has and will continue to work closely with all impacted employees and the Committee to facilitate a smooth transition. The CAO is also actively monitoring the effectiveness of the new standards and their operational impact on shared employees and their employing offices and will present the Committee with suggested modifications to the standards later this year.

To reinforce these new standards and other vital information security protocols, HIR regularly reviews and seeks Committee approval to revise the House Information Security Policies.

Migration of House-wide Applications to the Cloud
One of the largest HIR modernization efforts underway is the migration to cloud-based applications. House-wide cloud applications increase operational efficiency and workflow through expanded self-service IT solutions and improved service delivery speeds. Their House-wide deployment also saves offices money. With those benefits in mind, the CAO is constantly working to vet and deploy cloud applications to the House.

For example, the CAO is in the process of upgrading all House offices from Microsoft's Office and email applications to the latest cloud-enabled Microsoft Office 365 and Microsoft Outlook cloud-based email. Once fully operational, Members and staff will be able to securely access their documents and email from anywhere

44

using a House-issued device. They will also be able to collaborate with their colleagues in real-time and have five times as much storage space for emails and documents. The upgrade to Microsoft's cloud applications is expected to be completed in 2019. The standardization to a single licensed cloud version of Microsoft Office will also enhance network security and supportability while yielding cost savings for the House.

In addition to the migration to Microsoft's cloud applications, the CAO continues to review and approve other cloud applications for use by House offices. There are currently multiple popular cloud services approved and in use by the House community, including Box, Dropbox, LinkedIn Learning, SurveyMonkey, and EventBrite. The CAO is also implementing a cloud-based learning management system that will improve the registration experience for employee training and enhance the House's tracking capabilities.

The House Web Services team, which has developed two-thirds of House.gov websites, is migrating the House's public facing websites to the cloud to ensure resiliency and to provide a seamless development environment. Cloud hosting also provides greater access to the latest hardware, timely security patching and updating of software, and around-the-clock monitoring of the sites and infrastructure allowing House Web Services staff to focus more on customer-oriented development needs instead of routine maintenance and backend processes. Additionally, the cloud provides robust resiliency across multiple data centers – ensuring the websites are always available.

To date, House Web Services has migrated and is currently hosting all new freshman Member websites, House.gov, and a number of other websites on the cloud. Its goal is to have all CAO-hosted sites migrated to the cloud by July 2019.

Technology Recapitalization
As the House continues to increase its reliance on cloud applications, which optimize services, it must reduce its reliance on legacy technologies through recapitalization. Specifically, the House must look to offset IT hardware, software, and maintenance contracts at existing data centers. Though there will be a need to operate House data centers for the foreseeable future, the CAO can certainly cut back on the House's use of them and the associated costs, which are significant. With the uptick in cloud services, the CAO is actively working on a recapitalization plan for the House to scale down resources at existing data centers as appropriate.

Internet Bandwidth & Data Upgrades for D.C. & District Offices
Increased reliance on cloud-based applications and the internet in general also requires the CAO to make increasing bandwidth and improving data connections a priority – especially for district offices. In August 2018, the CAO upgraded its internet circuits from two gigabits to three gigabits at each of its internet border routers. The upgrade of the circuits increased House internet bandwidth by 50 percent for D.C. and district offices.

Since the beginning of the 115th Congress, the CAO has been actively engaged to

equip all the freshman district offices with Voice over Internet Protocol (VoIP) phone service. VoIP connections yield higher-quality data and voice connections, greater functionality, and cost savings. To date, 270 district offices are now either on the VoIP platform or are in the process of migrating over to the platform. During the 116th Congressional Transition, the CAO continued its effort to connect all freshman offices to broadband and VoIP platforms and is now focused on expanding VoIP to the remaining district offices.

During the 115th Congress, all 441 district office data connections were migrated to broadband technology. This new service allowed for faster interaction with the CAO services located on the D.C. campus, faster downloads of larger files, and improved video teleconferencing. On average, district offices experience increased speeds up to five times faster on downloads and two to three times faster on uploads. The migration to broadband not only enhanced the performance for district office staff, but garnered annual savings of more than $2 million.

With the $2 million in savings realized from the district office upgrades, the CAO invested in network and security infrastructure at a West Coast data center that will provide all West Coast district offices with the ability to access the internet locally. Under the current architecture, all West Coast district office data connections must travel across the U.S. in secure encrypted tunnels to D.C. to access the internet. Expected to be completed by the end of this month, the new architecture will deliver enhanced connectivity for all district offices located on the West Coast. Pacific offices, including those in Alaska, Hawaii, Guam, the Northern Mariana Islands, and American Samoa, are already on this new architecture and are experiencing increased speeds.

Identity and Access Management
Identity and Access Management (IAM) is a critical, multiyear program to improve controls over employees, contractors, detailees, fellows, and any other individual who may have access to House systems. IAM relates to how offices receive, update, and/or exchange identity-related information and use it to manage access to various House resources such as the House network, financial systems, and privileged accounts.

Improving and streamlining the House's IAM is critical to enhancing cybersecurity, securing personal information, and improving the efficiency of House business processes. To streamline the House's current IAM processes, the CAO created a dedicated Identity Governance and Administration organization in January 2018.

In May 2018, Identity Governance and Administration developed and deployed a new identity hub that integrates with My PayLinks and, as it continues to mature, will integrate with other House applications and identity sources starting with the House Sergeant at Arms' badging system. The goal is to create one system whereby the onboarding process for new hires includes adding information into the identity hub that triggers workflows to other CAO departments and House offices responsible for various aspects of the onboarding process such as badging and network account

creation.

Once complete, the IAM system will provide the House with a consistent, secure, and reliable House-wide program for identity management and will improve the technology related to the authentication, authorization, management, and oversight of identity and user access to House systems.

Simplified Online Access to House Systems & Services
To simplify and streamline access to the House's financial systems regularly used by Member, Leadership, and Committee offices to manage their respective office budgets, the CAO launched the new Financial Systems Portal in 2018. In addition to streamlining access to financial systems, the portal provides a quick overview of each office's finances and an enhanced user experience similar to modern online banking systems.

Additionally, to help offices quickly obtain the services they need, the CAO has continued to expand its online self-service tool – MyServiceRequests – that now includes 127 services. Since its creation, the self-service tool has grown in popularity with the number of monthly requests increasing from 350 in 2014 to 2,368 by the end of 2018.

Other Major Ongoing Initiatives
In addition to the above-mentioned customer service and innovation initiatives that align with the CAO Strategic Plan, the CAO is responsible, either in part or in whole, for executing other major ongoing House initiatives. However, as mentioned, all CAO employees and services have been impacted by the implementation of the Strategic Plan, including the initiatives outlined below.

Transition
Every two years, the CAO partners with the Committee on House Administration, the Clerk of the House, the House Sergeant at Arms, the Architect of the Capitol, and additional House stakeholders to ensure a smooth and successful transition to a new Congress. The transition to the 116th Congress built on this history of cooperation. From office moves, to website development, to onboarding new employees, CAO business units played an important role in the transition.

Representatives from a variety of CAO offices, including the new CAO Customer Advocates, participated in briefings to help departing Members wind down their operations and close their offices and help newly elected Members get their offices up and running. Working together, the CAO's technology and logistics divisions facilitated D.C. and district office moves and/or setups for returning and new Members as well as Committee and Leadership offices.

To support the 116th Transition, to date, the CAO:
- Facilitated 278 Member office moves
- Created 91 new Member websites

- Coordinated modifications to and/or modified over 30 Committee sites and 9 Leadership sites due to leadership changes
- Completed over 56,000 payroll actions
- Reviewed and approved approximately 825 district office leases

Cannon Renewal

CAO business units continue to support the Cannon Renewal Project now in its second phase. To support phase one of the Project, the CAO's Modular Furniture and Transition team designed and outfitted 31 Member offices, 2 Committee offices, the Clerk's Legislative Resource Center and office spaces, the Office of the Attending Physician's Health Unit, the ID office, conference rooms, and other ancillary spaces occupied by an estimated 1,500 employees. Additionally, the team partnered with the Architect of the Capitol to host three "sneak peek" sessions for those with Cannon offices to view the furniture layouts and answer questions. HIR also supported the first phase by installing the network and telecommunications infrastructure, including the installation of 414 VoIP phones.

To support the second phase of the Cannon refurbishment, Modular Furniture staff reached out to all affected offices to provide guidance and assistance on the upcoming mandatory move processes. HIR is also working with the Architect of the Capitol on network and telecommunications infrastructure design. Lessons learned from phase one of the Project have yielded improvements to phase two coordination and communication between the CAO and Architect of the Capitol. For example, the placement of various building fixtures will be relocated to better align with furniture plans.

Financial Services

The CAO's Finance division continues to implement the actionable recommendations to improve accuracy, accountability, consistency, and customer engagement provided by an independent firm in September 2017. For instance, it is working on the ongoing development of its internal policies and procedures and using in-house knowledge management technology for CAO employees to establish and share precedents and resolution experiences. The knowledge management initiative will aid in standardizing activities using the appropriate process, procedure, and policy documents. In addition, organizational insights will be preserved.

In October 2018, the CAO modernized the House's voucher submission process, transitioning to a completely digital submission process so offices can submit vouchers from anywhere at any time. Converting to digital submissions also increases voucher tracking capabilities and reduces the unnecessary use of staff resources and paper. The new digital process, which also allows CAO employees to accept and process vouchers from any location, promotes continuity of operations during emergencies or inclement weather events.

48

The Office of Finance is also working to implement the use of electronic signatures that will allow Members and staff to electronically complete, sign, and securely submit required financial forms. This modernization effort will save time and resources.

At the beginning of the 116th Congress, the CAO completed a successful transition to a new House Finance Card Program, which impacted all existing and prospective House Travel Card and Purchase Card cardholders and their financial administrators. The transition required negotiating a new credit card contract and issuing more than 1,000 new cards and account numbers. It also presented an opportunity for the CAO to improve internal House Finance Card Program policies, card issuance and payment processes, and training and certification requirements. For example, under the new payment process, all card transactions now load directly into the House's financial system so offices can create vouchers with just a few clicks, eliminating both time-intensive data entry and potential human error.

To increase understanding of the House's financial policies, processes, and its systems of record, the Committee on House Administration instructed the CAO to establish a House financial services curriculum for designated financial points of contact who are authorized to access the House financial systems and submit and/or approve financial actions. Working with the new Congressional Staff Academy, the Office of Finance has developed a two-part course curriculum to be delivered in person and online that will cover House policies pertaining to the use of official resources and mandatory financial procedures. It also includes in-depth, interactive systems training.

Wounded Warrior Fellowship Program

The House's Wounded Warrior Fellowship Program provides paid, two-year fellowships for wounded and/or disabled veterans to work for Congress. In 2018, the Program was expanded to accommodate 110 offices seeking participating fellows – more than doubling the size of the Program. The expansion is helping the CAO meet the increasing demand for fellows, illustrated by the Program's waitlist averaging over 100 House offices despite the expansion. Fellows are currently placed in 55 House offices, and the additional 55 positions are in varying stages of recruitment with 15 fellows expected to be onboarded in House offices before the end of May 2019.

Part of the CAO's expansion efforts included a robust education campaign to generate greater awareness of the Program and its benefits among Member offices. As a result, in 2019, the Program will realize record levels of office participation and diversity. Moreover, fellows will work in offices in more ethnically, culturally, socio-economically, and geographically diverse congressional districts.

Working closely with the CAO's new Congressional Staff Academy, the Program continues to improve professional development opportunities for participating fellows to develop and strengthen their transferrable skills. For example, in 2018, it launched a four-day orientation program for new fellows. Located in Washington, D.C., the orientation includes briefings from various Executive Branch agencies, all branches of the military, the American Folklife Center, and the Congressional Research Service.

49

This year, the orientation will be expanded to a fifth day, further enhancing the skills of new fellows.

To date, more than 250 fellows have participated in the Program, and more than 50 alumni of the Program have been permanently hired by House offices.

Asset Management
The House has over 60,000 accountable equipment items assigned to over 1,500 separate House office inventories. These inventories are spread across seven buildings in Washington, D.C., and over 900 district office locations. Approximately 30 percent of the inventory is over seven years old, and some items date back to the 1950s. The CAO is responsible for tracking all accountable assets. However, the autonomous nature of House office operations and equipment purchasing processes complicates CAO efforts to track, transfer, and dispose of House equipment, and deficiencies associated with asset management have been highlighted by House auditors dating back to FY13.

To address the identified deficiencies, the CAO has undertaken several initiatives to yield immediate process and accountability improvements and facilitate a phased approach to develop and expand its asset management practices to the entire House. Immediate improvements include the implementation of a more stringent review policy for the disposal of assets, the standardization of asset tagging and tag placement to inventoried items, and the deployment of network discovery technology that detects approximately 22,000 computer assets on a daily basis. The CAO is also actively working to improve House office inventory education and awareness through the creation of management guides, customized training, increased hands-on assistance through its Customer Advocates, and greater access to real-time office inventory data.

The FY17 House financial audit acknowledged the corrective actions taken in response to the House's previously reported internal control deficiencies and highlighted efforts underway to mature inventory policies and procedures, expand inventory processes to include capitalized property, and develop a risk-based approach to identifying inventory items and reviewing processes. With the continued development and implementation of the CAO's asset management objectives, the CAO is confident that the external auditors will identify continued improvement in the FY18 audit.

The CAO's long-term asset management goals were established using the results of a comprehensive, independent gap analysis completed in April 2018. The analysis entailed a thorough review of House practices, audit findings, and industry best practices. It included recommendations to improve the effectiveness of end-to-end inventory processes performed by the CAO and establish clear program goals and tools to measure success. Per the recommendations, the CAO began with internal changes to its practices and plans to systematically expand the practices to other House offices as necessary. The CAO is also exploring House-wide expansion of centralized receiving, developing a risk-based approach to defining and tracking assets, and further improving access to inventory information and support. Implementation of the recommendations is underway and slated to last through FY21.

50

Concluding Statement
Philip G. Kiko
Chief Administrative Officer

Since I last testified, the CAO has made significant progress with its prioritized initiatives, especially the implementation of its customer and innovation-focused Strategic Plan. Implementing the plan and its objectives has forced the organization to step back and reevaluate the services it provides, examine them through its customers' eyes, and determine the best way to deliver them.

I appreciate the opportunity to present these priorities on behalf of the CAO's dedicated employees and express my sincere gratitude for the Committee's support.

The CHAIRPERSON. Thank you very much.

And finally but not least, Mr. Ptasienski.

STATEMENT OF THE HONORABLE MICHAEL T. PTASIENSKI

Mr. PTASIENSKI. Good morning, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. I am both pleased and honored to appear before you today in my capacity as the Inspector General of the House.

I would like to briefly provide a little bit of background on our office and work before talking about priorities for 2019 and beyond.

Our core mission is to conduct audits of the financial and administrative functions of the House. Since the first Inspector General of the House was appointed in 1993, the OIG has worked closely with the House officers and those charged with oversight to improve the operations of the House, reduce inefficiencies, minimize costs, identify and prevent fraud, and mitigate risk. We provide traditional audit services as well as proactive analysis and guidance for improvement through our management advisory services.

The priorities for my office are largely driven by those of this Committee and the House officers. As new initiatives are undertaken, policies are updated, technology and/or process changes are made, the risks also change.

The House will face numerous challenges during the 116th Congress and beyond, some of which we know and others we do not. The OIG will continue to do our part to help the House officers and this Committee identify and manage risks wherever they exist. We are dedicated to making the House secure, safe, and more efficient and effective.

I believe our independent, data-driven audit and advisory work is critical to both the officers and this Committee as you work to prevent issues that could adversely impact the operations of the House and the legislative process.

At the direction of this Committee and in collaboration with the House officers we have revamped the audit planning process. This collaborative, transparent process involves discussions of risk, current and planned initiatives, and discussing existing operational challenges. We have these conversations with both the officers as well as the key staff that handle the day-to-day operations.

Through our regular meetings with Committee staff, we also discuss the concerns and priorities of those with oversight responsibilities. These planning discussions allow us to gather a much more comprehensive view of the House environment and form our risk assessment process. I believe this communication has also improved coordination between my office, the House officers, and this Committee.

We have submitted and reviewed our draft 2019 work plan with the Committee staff. It is a focused, risk-based audit plan that centers on critical aspects of the House administrative operations, legislative process, and security. I look forward to receiving approval on that plan so we can begin work on these important efforts.

For the foreseeable future, it is apparent that cybersecurity and ensuring the resiliency of House systems and infrastructure will continue to be an area of focus. Technology is ever-evolving and

continues to become much more embedded in all aspects of House operations.

While technology offers great efficiencies and can dramatically improve the delivery of information and services, it also expands the number of attack vectors for cyber attacks and creates new risks, where even a simple outage can disrupt key services.

In addition, the continued evolution of cloud services and applications offers a potentially limitless number of locations where both personal information and House data may reside.

Being able to quickly deploy and take advantage of new technologies while also ensuring that processes are in place to manage information security is both critical and an immense challenge.

Chairperson Lofgren, I wish to thank you, Ranking Member Davis, and Members of the Committee for the opportunity to appear before you today. I want to assure you that will we continue to provide our unbiased and independent assessment of risk, provide data-driven analysis, and offer practical recommendations to improve the effectiveness and efficiency of House operations.

At this time, I would be happy to answer any questions you have.

[The statement of Mr. Ptasienski follows:]

Statement of Michael Ptasienski, Inspector General
Office of the Inspector General
U.S. House of Representatives

Before the Committee on House Administration
April 9, 2019

Chairperson Lofgren, Ranking Member Davis and Members of the Committee, I am both pleased and honored to appear before you today in my capacity as the Inspector General of the House. I would like to briefly provide a bit of background on our office, the role we perform, and highlight a few items before talking about priorities for 2019 and beyond.

The OIG was established in the U.S. House of Representatives (House) by House Resolution 423 *"House Administrative Reform Resolution of 1992"* during the 103rd Congress. Its mission is to conduct periodic audits of the financial and administrative functions of the House and of joint entities. Since the first Inspector General of the House was appointed in November 1993, the OIG has worked closely with the House Officers, and those charged with oversight to improve the operations of the House, reduce inefficiencies, minimize costs, identify and prevent fraud, and mitigate risk. The OIG provides traditional audit services, as well as proactive analysis and guidance for the improvement of House operations through our management advisory services. Due to the importance of information technology and cyber security, the OIG continues to provide robust technology assessment and risk expertise to the House.

Over the past two years, the Office of Inspector General's (OIG) objective, value-added reviews focused on improving the House's financial and asset management, administrative processes, workplace safety and security, the security of House data, and the information technology infrastructure. During the 115th Congress, the OIG issued 22 reports, which spanned the diverse range of services the OIG offers including financial, performance, and information systems auditing services; and management advisory services.

Financial audits examine the accuracy, effectiveness, and efficiency of House financial operations. A major portion of this effort involves our oversight of an external certified public accounting firm's annual audit of the House financial statements. For the 20th consecutive year, the external auditors expressed an unmodified opinion on the House's FY2017 financial statements. An unmodified opinion is the best rating given by auditors. It states the House's financial statements present fairly, in all material respects, the financial position and results of House operations in conformity with generally accepted accounting principles. The external auditor did, however, report a repeat significant deficiency from the previous audit report, relating to the controls over property and equipment. Additionally, a significant deficiency was also reported relating to controls over financial statement presentation and disclosures.

The Office of Inspector General recommends the selection and oversees the contract with the external auditing firm. Every 5 years the House requests proposals from firms and recompetes the award of this contract. While changing auditors can initially be more time

consuming as new auditors become familiar with the operations of the House, there is a benefit to having a "fresh set of eyes" doing this work. For the FY2018 audit we have selected and engaged a new public accounting firm to conduct the external financial statement audit. This audit is currently underway, and we anticipate work concluding in the coming weeks and having the final report ready for publication this summer.

The House will face numerous challenges during the 116th Congress and beyond, some of which we know and others we do not. The OIG will continue to do our part to help the House Officers and this Committee identify and manage the risks that arise. We are dedicated to making the House secure, safe, and more effective and efficient. Our independent, data-driven audit and advisory work is critical to both the Officers and this Committee as you work to mitigate significant risks to the House. In doing our work, we also highlight any opportunities we identify that can improve the efficiency and effectiveness of House operations.

At the direction of this Committee, and in collaboration with the House Officers, the OIG has re-vamped the audit planning process. This collaborative, transparent process involves discussions of risk, current and planned initiatives, as well as existing operational challenges. We have these conversations with both the Officers and the key individuals that handle the day-to-day operations. Through our regular meeting with Committee staff, we also discuss the concerns and priorities of those with oversight responsibilities. These planning discussions allow us to gather a more comprehensive view of the House environment and inform our risk assessment process. In totality, this process has helped foster better communication and improved coordination with the House Officers and your staff.

We have submitted and have reviewed our draft 2019 work plan with the Committee staff. This is a focused, risk-based audit plan that centers on critical aspects of the House financial operations, legislative operations, and the security of life and property. I look forward to receiving your approval of that plan, so we can begin work on several important efforts.

For the foreseeable future, it is apparent that cyber security and ensuring the resiliency of House systems and infrastructure will continue to be an area of focus for us and for the House. Technology is ever evolving and will continue to become much more embedded in all aspects of the operations of the House. While technology offers great efficiencies and can dramatically improve the delivery of information and services, it also expands the number of attack vectors for cyber-attacks and creates new risks where simple outages can disrupt key services.

Technology continues to offer great opportunities to reshape how work is accomplished. Being able to quickly and securely deploy these tools is a big challenge. The continued evolution of cloud services and applications offers a potentially limitless number of locations where both personal and House data may reside. Being able to quickly take advantage of new technology while also ensuring that processes are in place to assess and manage the risk and underlying security of these services is critical. It is also an immense challenge for any organization, but the unique nature of IT at the House makes that even more challenging here. To successfully perform our work, we all need to make sure we have the processes, tools, and structure in place to attract and retain the necessary talent to do this type of work. Staff development and acquiring the Human capital with the necessary technology knowledge and skills is a challenge; one which we will have to overcome.

Chairperson Lofgren, I wish to thank you, Ranking Member Davis, and the Members of the Committee for this opportunity to appear before you today. I want to assure you that we will continue to provide our unbiased and independent assessment of risk, provide data-driven analysis, and offer practical recommendations to help mitigate risk and improve the effectiveness and efficiency of House operations. I firmly believe our work is critical in helping protect the House from financial loss, and delays and disruption to House financial and administrative operations. We look forward to continuing our role of providing value-added advice and counsel to this Committee and focusing on issues of strategic importance to the House. At this time, I would be happy to answer any questions you may have.

The CHAIRPERSON. Thank you very much.

And thanks to all of you, not only for your good work for this institution but for your testimony today.

Now is the time when members of the Committee may ask questions of the witnesses, and I am going to turn first to the gentlelady from California, Mrs. Davis.

Mrs. DAVIS of California. Thank you very much, Madam Chairperson.

And thank you for all of you who make the House a better place for those who work here and, of course, those who visit here as well.

My question is for Ms. Johnson and Mr. Kiko. I appreciate very much your willingness to work with me on an idea that we have had in my office to modernize the way that we add cosponsors to bills.

As you all know very well, legislative staff and interns are constantly calling and emailing around for cosponsors and running signed cosponsor sheets to the Capitol when, in fact, they certainly could be doing other probably more important work. The processing of lists of names takes several hours of Clerk staff time as the cosponsor sheets are handwritten and can be easily misread.

So there is really no good reason for our co-sponsorship process to be like this in 2019. It is neither efficient nor secure considering that there about 135,000 co-sponsorships every Congress, saving time here could certainly free up many hours of legislative and Clerk staff hours.

I propose that we develop a new electronic system that would provide offices with a checklist of bills that they can sign on to and bill sponsors with a way to collect names and let others know their bills are open for cosponsors. An online system could increase efficiency and accountability, as there would be an electronic record of authorized staff signing on to bills.

The creation of such a system would not be difficult but it certainly would require collaboration between the Clerk's Office and the CAO's Office. I wonder if each one of you, Ms. Johnson and Mr. Kiko, if you could tell me how you suggest we proceed and how the Committee can best support you as we explore this idea. What do you see as the next steps?

Ms. Johnson.

Ms. JOHNSON. I would recommend that we begin talking to the Parliamentarian's Office to make certain that we don't in any way impose on the integrity of the current system, which I don't see as a problem. We have started talking to our legislative computer people, and they are certain they can develop software to make certain this process is carried out efficiently.

I think it is a matter of changing the culture of the Members because they are very accustomed to doing it the old-fashioned, manual way. It would certainly benefit the Clerk's Office. We spend about 5 hours daily each day that we are in session between collecting the cosponsors, calling the offices back to make certain that the names are correct, and, even after that, just putting the data into the system of all the cosponsors. It is very, very time-consuming.

The Clerk's Office prides itself on reliability and efficiency, and so we will look into it and just make certain that nothing is lost in the process.

Mrs. DAVIS of California. Thank you.

Mr. Kiko, did you want to comment?

Mr. KIKO. We would be willing to assist the Clerk on the technology aspects if they need it.

I know from my own personal—and I guess some of this is about, you know, figuring out a way, on your idea, just to validate what is currently already happening. Obviously, staff is making calls, you know, putting people on. Maybe that would be really critical, to make sure the validation process up front is correct.

And so that is how I see it. I have worked on a personal staff before and I can attest to how difficult the process is and how it is time-consuming. We would be willing to assist the Clerk in any way we could.

Mrs. DAVIS of California. Thank you very much. I appreciate that.

Madam Chairperson, I certainly know how much time it takes in our offices. I had no idea how much time it took in the Clerk's Office.

The CHAIRPERSON. Thank you very much, Mrs. Davis.

I turn now to the other Davis on the Committee, the Ranking Member, Mr. Davis.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

And hello, Mr. Kiko. How are you today?

Mr. KIKO. I don't know. I will tell you at the end of this hearing.

Mr. DAVIS of Illinois. I see you brought your entourage back too. Mr. Clocker is having flashbacks to his time spent here.

Phil, what do you see as the biggest technology challenges that Member offices face right now?

Mr. KIKO. I think with regards to technology, it has to do with the interface sometimes with the Finance Office on how we interface on voucher processing. I think it has to do with an interface also just with regards to the computer requirements that we have, with regards to the IT requirements that we have.

I think that the challenge is basically because there is a tension between security with regards to our whole technology system that we have, and then we have these many devices that Members have and it is not a very centralized function. And I think there is frustration sometimes on the interaction on IT things with regards to the CAO's Office.

Mr. DAVIS of Illinois. Okay.

Mr. KIKO. Does that make sense?

Mr. DAVIS of Illinois. Yes. I wanted to get your opinion on that. You certainly had to listen to mine sometimes and we did last week. We had a great conversation on the technological backbone of HIR and how do we create more competition within our CMS systems to be able to help get Member offices the most up-to-date technology to be able to communicate with our constituents. I look forward to working with you and your team on those issues.

Mr. Kiko, it is my understanding that last year the CAO's Finance Office was reviewed by an outside consulting firm. What were the recommendations from that study and when will they be

implemented? And, most importantly, how are they going to help Member offices?

Mr. KIKO. Well, I think the recommendations—there were about 30 recommendations that had to do with a lack of written processes for the CAO operation. And they took a deep dive into everything we did. I think that we are to implement the recommendations and the processes—there were several, like 200 or 300, process recommendations in addition to other recommendations.

And we are supposed to have those implemented by the end of this year. I do think that it will tell employees in the various operations what they are supposed to do and how they are supposed to do it, written down rather than just in somebody's head and "this is the way we have always done it."

Mr. DAVIS of Illinois. Okay.

And I mentioned the Member offices. You and I and your team have gone through an office of finance review process. We updated some of the categories a few years ago. Thank you for your work.

Obviously, you know my viewpoint is, I view the CAO and the Office of Finance as somewhat of an insulation point for Members. I want to make sure you know that this Committee, all of us on this Committee are hoping to work with you to make sure that Members don't ask for things that get Members in trouble. We want to make sure that you have the tools that you need.

And that is why I am most concerned—and we can talk later. I want to know how these changes are going to help Member offices too——

Mr. KIKO. Right.

Mr. DAVIS of Illinois [continuing]. Not just help the Finance Office. Because we want to make sure—it is not just about voucher times, processing times. It is, what the end result? How are your processes going to make it easier for Member offices to work in conjunction with the Office of Finance?

Any comment there?

Mr. KIKO. No, I mean, I am trying, especially on the voucher processing, on making the processing time shorter.

Mr. DAVIS of Illinois. I understand that, but that shouldn't be our only focus. The voucher processing time is not the only focus.

Mr. KIKO. Right.

Mr. DAVIS of Illinois. That is, you know——

Mr. KIKO. Well, I think, overall, we are going to have more integrity in the system, and we are going to be able to rely on the system.

But with regards to, you know, the finance audit, we have been doing okay with regards to the auditors. But we need to do better, I agree, with regards to how we interface with Member offices and make things better and faster and less bureaucratic.

Mr. DAVIS of Illinois. Thank you.

Mr. Irving, thanks for your badge implementation. I don't have enough time, so I have to skip you.

Ms. Johnson, quick question. What steps is OHEC taking to proactively reach out and educate Members about best practices in workplace rights?

Ms. JOHNSON. We have a series of trainings. We are working in conjunction with the CAO's Office in training chiefs of staff, and we also offer trainings to Members on workplace rights.

Mr. DAVIS of Illinois. Okay. Thank you.

The CHAIRPERSON. Thank you very much.

I would like to recognize the gentleman from North Carolina for his questions.

Mr. BUTTERFIELD. Thank you very much, Madam Chairperson.

And let me say good morning to all of you and thanks very much for your testimony today.

In my prior life, I was a judge for some 15 years, and I would show up in superior court every Monday morning and have a courtroom full of people and full of defendants and full of lawyers, but I could not do my work without the court personnel. I was useless as a judge. As Members of Congress, we are—I am not going to say "useless," but we are marginalized unless we can have the support of men and women like yourselves.

I want to thank you very much for the incredible work that you do on behalf of all of us. And not just you. You are at the top of the chain, but you have many, many people who work with you and for you who give of themselves every day. I just want to ask you to extend to them our appreciation for all the work that they do.

This is serious work that we do here in Washington. We all know that. The Sergeant at Arms, I have really developed an appreciation for the incredible role that your office plays in the life of Members of Congress. I am not sure that the newer Members of Congress really understand and appreciate the depth of the work of the Sergeant at Arms, and, hopefully, as the years go on, they will develop an appreciation for it, as I have done.

I am always looking for ways to increase Member security without being ridiculous, and there is a fine balance between that. You know, whenever Members have an emergency in their lives—and we have known some over the last few years—we become very attuned to the risks that we face, but as time goes on, that kind of wanes and we kind of relax.

Many of us are from rural communities. I have 14 counties in my district. Some are urban; some are rural. I find myself, from time to time, on back roads late at night all alone, sometimes with staff, sometimes without staff. Sometimes the cell phone works, and sometimes it doesn't work.

I guess what I need to ask you, is there technology in place where you can locate a Member if there is an emergency? I know the technology exists. I mean, right on our phones, we can enable our devices to allow designated people to know where we are. And if we were to call you in an emergency, would you be able to—I know the police can do it as well. Can you identify where we are?

Mr. IRVING. Congressman, it is a great question. The technology does exist. We do have a system in place. It is a matter of us working closely with the individual Member so the Member is okay with us tracking their movements. That is the key. Is the Member authorizing us to——

Mr. BUTTERFIELD. Do Members know that? Do Members know that that capacity exists, that that technology exists? Because I

would be delighted for the Sergeant at Arms and the Capitol Police to be able to know my location in case of an emergency.

Mr. IRVING. It certainly is an ongoing education to the Members. I will say that Members all have cell phones, or most have cell phones, and with those cell phones we can track. We do have everyone's contact information so we do have the ability to certainly track them. Again, it is just a matter of ensuring that they are okay with that service.

Mr. BUTTERFIELD. Sure. But please—and I know you are going to do this, but please continue to remind Members of the incredible security risk that all of us face every day.

I think we heard from one of the other gentlemen about the hackers, the thousands and thousands of attempts being made every hour, I suspect, of people trying to infiltrate the workings of the House.

To Mr. Kiko, I didn't realize the severity of the bad actors—and I guess they are not just domestic; they are international as well—who are constantly trying to hack into our systems. Would you repeat that data again? I was caught by surprise. I knew it was a serious problem, but I didn't know the magnitude of the problem.

Mr. KIKO. Well, in just 1 month—I will read my statement——

Mr. BUTTERFIELD. Yes.

Mr. KIKO [continuing]. The CAO blocks an estimated 1.6 billion unauthorized——

Mr. BUTTERFIELD. Are you saying "billion," "B"?

Mr. KIKO. Yes.

Mr. BUTTERFIELD. Billion?

Mr. KIKO [continuing]. Probes, scans, and connections and 300 million to 500 million cyber-attacks each month.

Now, you know, on the first——

Mr. BUTTERFIELD. Is the trend line increasing, or is it flat?

Mr. KIKO. It is increasing.

Mr. BUTTERFIELD. It is increasing by the year.

Mr. KIKO. It is increasing. It is getting more intense and the actors are getting more sophisticated. The trick is for the CAO to stay ahead. We try to stay ahead of the curve. We have a lot of ways to try to block things from coming in.

Mr. BUTTERFIELD. I would suspect your office interfaces with the CIA and the FBI and the——

Mr. KIKO. Yes, we interface with all the law enforcement agencies, correct.

Mr. BUTTERFIELD. Even at the State level.

Mr. KIKO. At the State level if we need to, yes.

Mr. BUTTERFIELD. Okay.

In your testimony to the Legislative Branch Appropriations Subcommittee, you mentioned $2 million in savings was realized from district office upgrades. Is that accurate?

Mr. KIKO. Yes. And it has to do with the technology for VoIP, you know, and replacing it—you know, not replacing VoIP, but having a better, cheaper system in district offices than what they have. We have been working our way through that with new Members. So, overall, it has been a cheaper system.

Mr. BUTTERFIELD. Again, thank all of you for your incredible work.

I yield back.

The CHAIRPERSON. Thank you.

The gentleman from Georgia is recognized.

Mr. LOUDERMILK. Thank you, Madam Chairperson.

I appreciate all of you, what you are doing, and the time you are spending with us today.

Security, Mr. Irving, has been a key issue for your office especially over the past few years. We have had even some classified briefings on the increased security threats. Many of us have lived through some of those, like you and I. I like you, but I never wanted to spend this much time with you on an official basis.

But a couple of questions. I remember not long after the baseball shooting that Mr. Davis and I were out there on the field with, the policy was changed, apparently, where if there was a significant number of Members together that we were going to get security. Are we still doing that?

Mr. IRVING. Yes. Absolutely.

Mr. LOUDERMILK. Is there a magic number or formula that we use for that or——

Mr. IRVING. No. We ask Members to let us know when they are off campus——

Mr. LOUDERMILK. Okay.

Mr. IRVING [continuing]. And let us make the determination. Frankly, I would rather know when Members are off campus and make that decision.

Mr. LOUDERMILK. Okay. All right.

You also mentioned that you are enhancing local security back in the districts for different events and coordinating with law enforcement, and you mentioned even having Capitol Police potentially come. What is the trigger mechanism to determine when you are going to bring a Capitol Police Officer in the district?

Mr. IRVING. A host of factors. We first will solicit local law enforcement support. They are the ones who can respond the quickest and have the most assets in the district.

Mr. LOUDERMILK. Right.

Mr. IRVING. If we feel comfortable with local law enforcement support, we will leave it at that.

If for some reason local law enforcement cannot support the Member event, then I will authorize the Capitol Police to deploy to the district, again, depending on the event and whether I see the risk is such that we need to send additional law enforcement.

Mr. LOUDERMILK. Okay.

The other question is regarding the implementation of the enhanced screening in the parking lot that is going to be done this year—or in the parking areas.

What changes would we see, operationally, for us? I mean, would that put us in a situation where access to the Capitol is more like it is in Senate? Or will we have fewer areas of ingress into the building from the parking areas? If you could just kind of touch on what changes we would see after this is implemented.

Mr. IRVING. Yeah, the real positive change I see is that the screening on the House side will be similar, almost identical, to what we see on the Senate side, which is no magnetometer screening from the Capitol to the Senate office buildings.

Mr. LOUDERMILK. Okay.

Mr. IRVING. I foresee a day where there is no magnetometer screening and much more free flow of staff. Members, obviously, bypass the magnetometers, but much more of the free flow of staff that are many times with a Member from the House office buildings to the Capitol.

Now, on the House office building side, there would be some business process change. As staff enter the garages, we will ask them to be screened at that point, similar to them screening from the street. Now, all pedestrians coming into the House office buildings will be screened, and that will, again, alleviate the concern of additional screening into the Capitol.

Mr. LOUDERMILK. The staff-led tours would not have to go through the magnetometer in the Cannon tunnel per se once it is——

Mr. IRVING. Technically correct.

Mr. LOUDERMILK. Okay. Thank you. I think that will be a great enhancement.

Mr. Kiko, you and I have discussed this in the past, and I just want to ask—and Mr. Irving can weigh in, too, if it is an area of concern there. Mine is dealing with the district offices and cyber—not district offices but Members' home offices and cybersecurity.

I see, coming from the IT background, that one area of weakness is just someone at home goes to Walmart or any other business and buys an off-the-shelf router that the password is "password," they put it on with their cable system, and all of a sudden now somebody driving down the road can get into their local network.

Is that something that is being addressed? Is there something to look at best practices or some training of how to best secure your homes?

Mr. KIKO. Well, I would say that all the practices that we ask Members to do here on campus are applicable to what you do at home. You know, whether it is changing passwords, you know, we will sit down and talk to you about how to best do that. We have done that with other Members.

We are going to have some kind of a fair coming up, I think, in a couple of weeks—and I will send that out—where it is basically a bunch of people in the cyber world meeting with Member offices on this particular issue. It is Members, you know, their offices, and these kind of things.

It is basically the same practices that we try to do here, but it is more difficult with regards to what you do at home.

Mr. LOUDERMILK. Madam Chair——

Mr. KIKO. Does that make sense?

Mr. LOUDERMILK. Yeah, it does.

I saw the Inspector General was nodding his head. I didn't know if you had maybe some comments on that as well.

Mr. PTASIENSKI. I would agree. The practices that are in place here at the House would be wholly applicable to Members working from home or from their offices. Some of the toolsets that the—if they are using VPN technology to get in, there is some degree of security that goes in there.

But, also, on the back end, those threats that the Chief Administrative Officer blocks all the time, they come from a variety of

sources. And now we have many more endpoints than we used to and IP-enabled devices. So my advice to Members would be: Be cautious anywhere you are, if you are in a hotel, if you are at home working. There really aren't safe locations to do your work.

Mr. LOUDERMILK. Thank you.

Mr. KIKO. I just want to say one thing. One of the biggest areas that we have where computers are ruined is people opening up phishing emails. And that would be one thing at home, which is hard to do because you get so much, but that would be the first one. If you don't know who is sending it, don't open it up.

The CHAIRPERSON. Thank you.

The gentleman from Maryland.

Mr. RASKIN. Thank you, Madam Chairperson.

Mr. Kiko, let me start with you. It was a pleasure visiting with you the other day.

I want to follow up on Mr. Butterfield's question about the numbers of cyber intrusions and attacks we are fending off every day. I was also staggered by those numbers. I just couldn't believe we are dealing with hundreds of millions or billions of attempts a year.

My question is, are we just playing defense on that? In other words, are we just trying to screen them out? Or do we actually go after the people who are doing it and attempt to prosecute cases and figure out where it is coming from?

Mr. KIKO. Well, we are in constant communication with law enforcement agencies on this matter. As was indicated earlier, a lot of these are from nation-states, and so that presents a different scenario and different complications.

But some of it is just, you know, when they do the probes and they do the scans, and then they will see where some vulnerabilities are. Then they will try to do the probe, and then they will try to get in so this is sort of a constant kind of thing.

We do work with law enforcement where we can, but a lot of it is just, you know——

Mr. RASKIN. Yeah.

Mr. KIKO. It is so hard. A lot of it starts in the dark web, and, you know, it is just hard.

Mr. RASKIN. You have described in your testimony the CAO's efforts to expand access to cloud services, like Microsoft Office 365, which would allow Members to access email and Word documents, Excel spreadsheets, other Members, and so on, all by using a House-issued device.

And we obviously use a lot of PDF documents here in the House. That is the standard file format for final legislative text, for constituent casework. Is there a CAO effort underway to examine the feasibility of House-wide access to cloud services that will support PDF documents?

Mr. KIKO. I would have to check on that. Hold on.

The answer is yes.

Mr. RASKIN. Good. Okay. Because I think that would——

Mr. KIKO. We will follow up with you on that.

Mr. RASKIN. It would make our lives a lot easier. Thank you very much.

Ms. Johnson, let me come to you. Do you have the resources and personnel in place to achieve all the goals of your office that you have developed?

Ms. JOHNSON. At this time, I do. I certainly have the resources in place.

My concern is that this area is just such a competitive technological area, and I concern myself with our salaries being able to keep up with IT salaries in the area and particularly with the oncoming of Amazon in the area. About a fourth of the Clerk's Office work staff is IT. I am just concerned about the competitive salaries.

Mr. RASKIN. I got you. Okay. Well, that is something that we will keep our eye on, too, then.

And is it true that you are a resident of Maryland's Eighth Congressional District?

Ms. JOHNSON. You are my Congressman.

Mr. RASKIN. Well, that is wonderful. Well, a special welcome to you.

I have just a final question for Mr. Irving—a couple questions.

One, what is the significance of prescreening Members, staff, and visitors to the Capitol complex, Mr. Irving?

Mr. IRVING. We employ the concept of prescreening to attempt to encounter a problem as far outside an office building as possible. We don't want the security issue to be inside. And if our prescreeners can identify a problem and hopefully neutralize a problem outside, we feel it puts us at a far advantage versus, again, inside an existing secure perimeter.

Mr. RASKIN. I got you. You have procedures in place for that prescreening process?

Mr. IRVING. Yes. And we do this because the campus is so open. We really attempt to balance the openness of the campus with security. And one way to put the advantage on our side, with such an open campus, is to push out our security to be able to identify things before they get to us.

Mr. RASKIN. Okay.

And, finally, Mr. Irving, I think I raised this with you when you were kind enough to drop by my office. Those of us who are on the House Administration Committee have two sets of constituents. One is our constituents back home, and then, by virtue of being on the House Administration Committee, our colleagues become constituents, in a way.

And I wanted to ask your help with a recurring constituent complaint I have gotten from some of my colleagues. And this is just about the hours of the House garages, specifically the Cannon garage, where I have heard a number of Members say they could be waiting 15 or 20 minutes before they leave because they have to go radio and ask someone else to come over.

I am just wondering whether we could work on extending the hours of the House garages for Members who work late. I mean, it seems to me like midnight would be a reasonable time to go. A lot of Members, you know, will be here for, you know, dinner meetings and events and late-night caucuses and so on. And I just wonder whether that is something we might be able to explore.

Mr. KIKO. Absolutely. We will certainly look into it.

We end up really balancing the number of Members utilizing those doors with the cost for the Capitol Police to staff them. But having said that, we want to make sure that every Member has access to the garage when they need it.

I commit to working with you on that, and I promise I will follow up.

Mr. RASKIN. Thank you very much.

I yield back, Madam Chairperson.

The CHAIRPERSON. The gentlelady from Ohio is recognized.

Ms. FUDGE. Good morning. Thank you all so much for being here. Thank you, Madam Chairperson.

As I have read and listened to your testimony, I really do see some commonality of purpose between your various offices, especially as it relates to systems. You are concerned about your security of the system and the efficiency of the system.

Do you all ever talk to each other about your systems? Because maybe they could work together better.

Mr. KIKO. We have frequent meetings all the time——

Ms. FUDGE. That is great.

Mr. KIKO [continuing]. Among the officers and frequent meetings with the IG.

Ms. FUDGE. The four of you get together on a regular basis?

Mr. PTASIENSKI. We do talk.

Ms. FUDGE. That is great to hear.

Just for each of you, what are the top two things that you would like to make sure you accomplish by the end of this Congress? And what do you see as the priority and vision for your offices for the next 5 years?

Ms. JOHNSON. I will go first.

I would say one of the top priorities is just to continue to recruit the best and the brightest staff from a very diverse pool of highly qualified applicants. We are working—whenever we have an opening, we are certainly consulting with the new House Inclusion and Diversity officer as well as working with minority-serving institutions and HBCUs. Number one is just, again, to have the best talent available and to recruit and retain that talent.

And, again, secondly, I would say just being able to be competitive with salaries. I am just afraid people are not going to stay unless they are paid a good wage for this area.

Thank you.

Mr. IRVING. I would say my two biggest priorities in the short term for this year would be the garage security project, to ensure that our House office buildings are within the secure perimeter, and the second would be to finish our Joint Audible Warning System to ensure that we have true redundant communications in the case of an emergency and we need to evacuate the premises or tell Members to go some other place other than their office.

In the next 5 years, I would focus on the districts and try to be more consistent with our protocols in the districts. As Mr. Butterfield indicated, I would like to ensure better coordination with all the Members with regard to the tools that we have at our disposal to keep them safe and ensure that Members take advantage of all of those tools.

Ms. FUDGE. Would that include continuing to put resources in our MRA for security in our district offices?

Mr. IRVING. That would be one, but I don't want to over-speak on that, but——

Ms. FUDGE. Right.

Mr. IRVING [continuing]. Yes.

Ms. FUDGE. Thank you.

Mr. KIKO. I would say that my biggest priority is to—we started a strategic plan a year ago, and it is about customer, process, stewardship, and employee. And if it is successful, it will basically transform how delivery of services are made to Members. It will be faster; it will be better.

And so that is sort of what my focus is, as far as in the next 2 years and beyond. I don't want to just deal with what is in front of me. I want to have the CAO's office, let's say, at the end of this Congress, to where it should be for the next 10 years, you know?

And the other one is a focus on professional and engaged CAO employees. Development of employees, training employees, upward mobility of employees—it has to do with that.

Ms. FUDGE. Thank you.

Mr. PTASIENSKI. Congresswoman, from my perspective, near term, some of the things that we are looking at or planning to look at have to do with technology resiliency and disaster recovery. It is an area that, with the amount of change and new technologies being brought into play, making sure that we are helping validate that the House is as resilient as it needs to be in case something bad were to happen, be it natural, unintentional, or deliberate or outside.

I think, longer term, I share some of the same concerns as the House officers, and that is making sure that the House—that we can get the talent that we need for our positions. As the Clerk noted, you know, with Amazon moving across the river, again, it is an additional entity that we will be competing with for talent, and particularly in technology areas. Making sure that we bring in the right people and can retain them and train them, I think that is a longer-term issue that we are going to have to continue to address but one that is, I think, going to become very, very important.

Ms. FUDGE. Thank you very much, Madam Chairperson.

The CHAIRPERSON. Thank you very much.

Just a couple of closeout questions.

First, thank you all for your testimony and for what you have done here today.

Looking at what the House institutionally has to offer Members and what Members understand about that is sometimes disconcerting. For example, HIR technology partners, I think, only has about 30 Member offices, if I have been told correctly, and yet it is—I have used it, it is a very efficient service and Members are spending money needlessly for outside vendors.

So the question, Mr. Kiko, is, how aggressively are we marketing—I guess, is that the right word?—to Member offices the IT service support? Are there cybersecurity benefits to having more Member offices supported exclusively by the HIR technology partners? And if so, what are we doing to increase the uptake?

Mr. KIKO. Well, we do have a marketing team, and we are going to be marketing those kind of services.

I think that, in the past, some of those services have not been very well-received. And I am not going to judge that, but, you know, once you get off on the wrong foot, sometimes it is basically hard to dig yourself out.

So what we are trying to do is increase, you know, the training, increase the people that we hire, increase how they interact with Member offices. And we are pitching the service with the customer advocates, you know, that we have hired to circulate around the Member offices.

I am sort of hoping the combination of all those will be better, because I think, from a security perspective, we would prefer that our people be working on the system.

The CHAIRPERSON. I would love to work with you on that, and sometimes Members can market to other Members. But if we are going to do that, I think we are going to need to incorporate the feedback from Members and then to you for corrections if there are things that people are unhappy with. You only get one chance to make a first impression.

Mr. KIKO. That is right.

The CHAIRPERSON. On the cyber issue, our policy is that critical updates have to be installed within 10 days, which I think is actually a pretty long—too long a time, and that noncompliance will result in disconnection from the House network. That is, I think, our policy.

Has that been enforced? And if so, how quickly? And what has been the feedback?

Mr. KIKO. Well, I think that I would have to defer, you know, on this, but it is my impression from what I know that we try to enforce those policies, but sometimes it is very difficult to enforce policies, especially dealing with a bunch of Member offices, and there is a lot of noncompliance.

And what we are trying to do on some of this stuff is, if we move into the cloud, we can automatically——

The CHAIRPERSON. You do it yourself.

Mr. KIKO [continuing]. Do it ourselves. And then that takes that off the table.

The CHAIRPERSON. I am going to follow up on an issue we have been working with you on. The National Institute of Standards and Technology is the gold standard on technology in the Federal Government. And they apparently have suggested that, instead of changing passwords constantly, it would be better to have an extremely long and complicated and secure password that is not necessarily changed a lot.

And you can go into any office and you will find by the Member's computer the password written down because they can't remember it. I think, you know, human behavior being such, we have been looking to move to that. Where are we on that?

Mr. KIKO. Well, I think recently we have changed, you know, the passwords to six characters, and you are only going to have to change them once a year.

And once we implement the multifactor, you know, in the next couple of months with regards to mobile devices, and once we move

to it, you know, at the end of the year so everybody can access it from their mobile devices and their desktop, I think that you could have that long password at the beginning when you enter it in but then, after that, you are not going to have that.

The CHAIRPERSON. Very good.

Mr. KIKO. That would be the way to go. But we can engage you further on that.

The CHAIRPERSON. That would be great. And it is one of the things that Members complain about, constantly changing it. And, really, because of human behavior, you end up with a less secure system because of people, you know, sending emails with "password" as the——

Mr. KIKO. Correct.

The CHAIRPERSON [continuing]. Tagline.

Mr. Ptasienski, in your answer to one of the questions—I think it was, what is your, kind of, work effort for the coming year—you talked about the IT strategies.

When was the last time the inspector general did an IT analysis of the House? And do you think that is something that would help us improve our IT landscape?

Mr. PTASIENSKI. We are constantly looking at various aspects of IT within all the House officer organizations. With Mr. Kiko and his organization, we spend a lot of time with HIR.

I am not sure if you mean holistically how we handle IT or what aspect you may be concerned with, but I am more than open to working with you and the staff to—if there are some specific concerns or areas, we can definitely——

The CHAIRPERSON. Great.

Mr. PTASIENSKI [continuing]. Look into those.

The CHAIRPERSON. I will just close with this. Rather than get the answer here today, I am wondering if I could ask you to submit to us your progress on diversity in hiring, what your plan is.

As you know, we are establishing a diversity office here in House Administration. But one of the things we want to make sure is that, you know, the employees of the House look like America and that we have made every effort to make sure that we have an excellent and diverse workforce.

And if you could, offline, submit what you are currently doing, what your plans are in that regard, it would be greatly appreciated. And then we will have an opportunity to have a further dialogue.

And with that, I see I am the only member of the Committee left, so I will thank you for being here today and note that we will adjourn. Thank you.

[Whereupon, at 11:09 a.m., the Committee was adjourned.]

Questions for the Record
Committee on House Administration Hearing
"House Officer Priorities for 2019 and Beyond"
April 9, 2019
The Honorable Cheryl L. Johnson, Clerk of the House of Representatives

Majority Question 1: Is the current organizational structure one you feel confident can meet the challenges ahead or are you contemplating any reorganizational efforts?

I am confident in the Office of the Clerk's ability to meet the challenges we face and will face with our current organizational structure. I am not contemplating any reorganizational efforts. Should that ever change, I certainly would consider appropriate reorganizational efforts.

Majority Question 2: Do you have the resources and personnel in place to achieve the goals of your office for this year and the year to come?

Our requested budget for FY 2020 would enable us to meet our goals. Areas of particular budgetary focus are ensuring we continue to have the resources to meet this Congress's hearing and oversight needs, fill the new positions described in my written testimony, and remain competitive in an increasingly challenging job market.

Majority Question 3: How does the Clerk's Office intend, in the coming years, to work toward achieving a more diverse workforce while ensuring that specialized, institutional skills are carried forward?

It is very important to me that the Office of the Clerk's staff be diverse and highly skilled. It has been my observation that we currently are both of those things. At the same time, it also is very important to me that we continually improve our performance against each of those measures.

As I noted in my written testimony, we will continue to develop our existing staff and recruit highly qualified new employees and will reach out to a diverse pool of applicants. I will ask my managers, as they think about staff development, retention, and recruitment, to continue to do so with both these goals in mind and to invite the ideas of their staff on these topics.

We also will continue to utilize all available House resources, including working with this Committee and your Director of Diversity. I look forward to an ongoing dialogue with the Committee on this critical issue.

Majority Question 4: At the end of your time as Clerk, where would you like the Office to be in terms of its functions, and what three things would you like to be remembered for?

I hope that at the end of my time as Clerk, we will have continued to ensure the integrity and modernization of the legislative process and improved public access to House Floor and Committee proceedings; supported the work of House Committees; and supported our outstanding staff to enable them to continue to flourish in their jobs and fully support this institution.

The three things I would like to be remembered for are (1) that I recruited and retained a diverse and highly skilled workforce in a competitive job market; (2) continued and enhanced collaboration and a close working relationship with the other House Officers; and (3) promoting technological advancements in support of the House's work, particularly modernization of the Legislative Information Management System (LIMS).

Majority Question 5: The STOCK Act mandated the creation of an online financial disclosure filing system for filers in the legislative branch. Your office created and administers the online system for filers who are Members of or candidates for the House, as well as House officers and employees and filers who are employed by certain other legislative branch offices. You indicated in your written testimony that you continue to "improve both the filing system and public access to records on our website," in close collaboration with the Ethics Committee. What improvements are you currently pursuing? With the benefit of six years administering the online filing system, as well as intervening changes in technology, are there any other aspects of the filing system and/or public access to the records on your website that need to be updated or changed?

In the current year, we are in maintenance and support mode and not pursuing major enhancements.

The financial disclosure system has been extremely reliable since its launch in 2014. Each year we meet with Committee on Ethics representatives to discuss areas of improvement and changes to the financial disclosure filing system. Most

change requests are executed and made available for the subsequent annual filing date.

Majority Question 6: In your written testimony, you indicated that since the online filing system was implemented, the percentage of filings made using the online system has increased "from 68 percent of filings in 2013 to 87 percent in 2018," which is impressive. Are you aware of any concerns or challenges that prevent filers who continue to file on paper from using the online system? If so, how do you anticipate addressing those challenges?

We believe that some filers simply prefer filing paper forms to online forms, in part because paper filers can add attachments. However, we believe that the percentage of online filers will continue to increase.

Majority Question 7/8: When has the online system typically been made available in advance of the annual May 15 filing deadline? Would additional resources or information from other House offices help your office make the system available to filers sooner? To the extent that it may be necessary to receive and analyze payroll data to assess which employees may be required to file, would it be feasible to make the system available earlier to Members and staff whose obligation to file is already known while the analysis continues for other potential filers?

Since its adoption, the online filing system typically has been made available each year as of the first or second week of April.

Regarding the remainder of this question (and your parallel question included in Question 9), given the multiple parties involved with the administration of the financial disclosure system, it is difficult for us to reliably make recommendations at this time that would impact and potentially have to be executed by parties outside the Clerk's office.

However, we share your desire to ensure that the system is available to filers as early as possible and is otherwise efficient and would welcome the opportunity to work with this Committee, as well as the Committee on Ethics, to identify appropriate options for achieving that goal.

Majority Question 9: When and how does your office notify new Members and staff about the fact that they are, or may be, subject to financial disclosure filing obligations? Would additional resources or information from other House offices help your office make these notifications sooner?

New Members are required to file their annual financial disclosure forms on May 15 and are notified by email on the same day as all other Members of Congress that the filing system is available. New staff who are hired at or above the "senior staff" compensation rate must file their financial disclosure within 30 days of receiving notice (by email) that they are subject to the filing requirement.

See also response to previous question.

Majority Question 10: Do you have sufficient staff and resources to continue administering the system as it exists today? Would additional information and/or resources from other House offices assist you in administering the online filing system and/or public access to reports? If any additional updates or changes to the filing system and/or public access were to be considered or implemented, would you need any additional resources to undertake them?

Maintaining sufficient staff and resources has been challenging. Additional staff and resources would enable us to reduce the burden of supporting multiple disclosure systems and would be necessary to support major improvements or changes to the system.

Majority Question 11: Please update the Committee on the status of your presence at the Redstone-Turner datacenter.

As of April 18, 2019, our backup data center presence at Redstone-Turner was fully operational for all Clerk systems. We no longer utilize the Alternate Computing Facility as a data center for any Clerk systems.

Majority Question 12: Please update the Committee on the status of the BioGuide and BioGuide Content Management system. Your predecessor advised the Committee that it anticipated completion would be the end of the second quarter of 2019, is that still the timetable?

The BioGuide Content Management System (revision 1.0) will be ready for deployment by the end of the second quarter of 2019. However, the public-facing BioGuide website launch will be delayed to the end of the third quarter to give us additional time to standardize the format of the Member biographical data from the old repository.

Majority Question 13: The Cannon Basement is an underappreciated space of the visitor experience to the Capitol complex. Please discuss your work on the Rotunda exhibits and provide the Committee the latest timetable for installation of the exhibit.

The Cannon basement rotunda is a major intersection of work and tours, a hub between buildings and the gateway to the Capitol for constituents taking staff-led tours. As part of the Cannon Renewal Project, we are installing permanent exhibition cases in the space, to provide a point of interest for constituents and other visitors to the House.

The initial exhibition, "How the House Works," will expand on what research shows is visitors' single biggest surprise when they visit the Capitol - that this historic building is also a working complex. More than 100 historic artifacts (from early 19th century House Chamber desks to early 21st century BlackBerries), documents, and images will tell visitors stories of how the variety of work in the House is done by and for people like them.

Installation begins May 20 and will be completed by June 7. An exhibit app and mobile website will launch at the same time, to support staff who are leading constituent tours.

Majority Question 14: In the Committee's oversight plan for this 116th Congress, we note that we will review the printing needs of the Clerk to evaluate the potential for eliminating duplication. Have you reviewed the printing requirements of your office and do you recommend eliminating any printed publications at this time?

Due to the unique nature of the items created by the publications team within our Documents and Requisitions section, and their role as the primary source of the information they contain, we have no duplication with other departments; therefore, we would not recommend eliminating any publications that we create internally.

Although we have not eliminated any printing publications completely at this time, we have reviewed the number of documents printed by the Government Publishing Office (GPO) at our request versus the number of documents we print on-demand and have relied increasingly upon our own on-demand printing to fulfill our needs.

Questions for the Record
Committee on House Administration Hearing
"House Officer Priorities for 2019 and Beyond"
April 9, 2019
The Honorable Cheryl L. Johnson, Clerk of the House of Representatives

Minority Question 1: What have your initial observations been of the Clerk's operation?

My primary observation is that the more than 200 staff that make up the Office of the Clerk have an unwavering commitment to working hard and with great professionalism to support the mission and goals of the House as an ongoing institution. I am deeply grateful for that commitment, and of course, share it. I will do everything I can to ensure that our staff continue to have a positive work environment that supports them and their professional needs.

Minority Question 2: What areas are going to be of focus to you?

I intend to focus on continuing the diverse ongoing activities of the Office of the Clerk as well as various special priorities and points of emphasis that I described in my written testimony – always with the highest professionalism.

These special projects include, among others, the JACK Act, the comparative print project, the Consensus Calendar, the BioGuide, LIMS, the Electronic Voting System, storage for Congressional records, high-speed printing, and the possibility of other lobbying disclosure enhancements. We will also continue to recruit, hire, and support a diverse, highly qualified workforce, and, of course, support the Cannon renovation.

I will also focus on the office's continuing ability to nimbly and successfully respond to unforeseen contingencies.

Minority Question 3: House rules require non-governmental witnesses appearing before any committee of the House to disclose recent grants or contracts from the Federal or foreign governments. That format often results in witnesses' hand writing their information on the disclosure form. Has any progress been made to develop and make available to all committees a disclosure document in webform to ensure the required information is typed and clearly readable?

Yes, the Truth in Testimony form is a witness disclosure document completed by

*witnesses appearing before committees in accordance with Rule XI, clause 2(g)
(5), of the U.S. House of Representatives. The form is uploaded to the Committee
Repository by committee staff on https://docs.house.gov, according to standards
set by this Committee and applicable House rules.*

*The creation of a standardized Truth in Testimony form was initiated at the request
of the House Appropriations Committee as part of the FY 2019 Appropriations
cycle. The report language can be found in House Report 115-696, accompanying
the Legislative Branch Appropriations Bill, 2019.*

*To comply with the report language and provide a solution at the start of the 116th
Congress, the Clerk's office created a standardized fillable PDF form. The
standardized PDF form was made available to all committees at the start of the
116th Congress (January 2019) on the internal HouseNet website.*

*This standardized fillable PDF form provided to the House committees and
subcommittees meets the requirements of the House rules and satisfies the request
in the Legislative Branch subcommittee report with the following guidelines:*

- *The form is completed by invited witnesses electronically, rather than by
  hand.*
- *The form is available to committee staff on https://housenet.house.gov.*
- *Form instructions, information, and training are provided to committee staff
  by Clerk staff informally or ad-hoc. Formal training is available as part of
  the Clerk-sponsored and Clerk staff-led Committee Repository training
  classes held at the Congressional Staff Academy.*

*To create the form, Clerk staff received input from this Committee and other
committee counsels to gather initial requirements and information. Following
that, all committees were invited to a meeting in fall 2018 to review the draft form
and provide feedback. After the form was made available in January 2019,
committees made minor change requests to the form. Clerk staff implemented
those change requests, and again, made the form along with instructions available
on HouseNet.*

*At this time, committees are not required to use the standardized form, although
many committees are providing it to their witnesses. The form can be completed
electronically and provided to committees for posting on https://docs.house.gov.*

Following are links to a sample form and the instructions.

Form: https://housenet.house.gov/sites/housenet.house.gov/files/forms/TTF.pdf

User Guide:
https://housenet.house.gov/sites/housenet.house.gov/files/documents/TTF-User-Guide.pdf

Minority Question 4: Your office's staff was largely impacted by Phase 1 of the Cannon Renovation project. Now that many of your staff have moved back into the Phase 1 space what has their feedback been?

With all moves associated with the end of Phase 1 of the Cannon Renewal Project now complete, the Office of the Clerk has moved approximately 50 staff members into newly renovated Cannon office space. These moves began in December of last year and the final move was completed in mid-March. While these moves were delayed from the original time frame and had to take place during the transition to the 116th Congress, which is a very busy time for our offices, staff from the Architect of the Capitol and the Office of the Chief Administrative Officer (CAO) worked hard to support us and the challenges we faced during these moves and we have been able to get everyone into their new spaces without negatively impacting the important work they do to support the House. From the reports I've heard from Clerk staff, they enjoy their bright, newly-renovated spaces.

Minority Question 5: Ms. Johnson, given that the primary mandate of the Clerk's office is to support the Legislative Process and the CAO office is to provide support services, how effectively does the Clerk's office utilize the specialized services provided by the CAO in terms of IT maintenance, specialized cyber security services, and advanced IT planning?

The Clerk's Office of Legislative Computer Systems (LCS) maintains a close working relationship with various divisions under the CAO and utilizes a wide range of CAO IT services and expertise to support our mission. We participate in a number of CAO technology working groups and utilize CAO enterprise license software, such as Windows and Office 365, to support the business and IT security needs of our organization.

Because of the critical role that Clerk IT systems play in supporting the legislative processes of the House, the availability and functionality of these systems against all risks is of paramount concern to me. As a result, Clerk LCS staff are directly

responsible for the development, maintenance and security of these systems. That said, we rely heavily on the CAO IT security staff to ensure a secure House network, to provide us guidance on IT security matters, and to conduct audits of new Clerk systems and equipment. Whenever possible we utilize CAO-provided technology to help protect our public-facing websites. We also work very closely with the CAO's Asset Management group to ensure that our Clerk equipment is properly handled upon disposal to appropriately protect House information.

Minority Question 6: Your FY 2020 budget request asking for $3.12 million to fund the next phase of the multi-year modernization plan of the House Legislative Information Management System.

a. Can you briefly summarize this project?

The multi-year modernization project for LIMS seeks to build a flexible system that can address every component of a bill's history. The system will be more flexible and create cost savings because the outdated code that supports the system will be updated.

b. How many phases are left and what do they entail?

We are currently in Phase II using previous no-year funding to cover costs associated with this phase. There are three phases remaining (III, IV, and V).

Phase III will be comprised of development of the core backend system components such as creating a user management module, a messaging platform, a workflow engine which is flexible and configuration-based, as well as a user interface stylesheet which will be used throughout the application and application data modeling. In addition, design and development will begin on individual LIMS modules and analyzing data migration requirements, as well as moving legacy data to a new platform and performing quality assurance and testing. The individual LIMS modules will include: Floor Action Reporting System (FARS), Committee Action Reporting System (CARS), Executive Action Reporting System (EARS), Reports Due to Congress, and Senate Action Reports (SARS).

Phases IV and V will include data modeling, user acceptance testing, running parallel systems as well as Alpha and Beta systems testing, and then a full production launch.

c. How will this benefit the House and specifically Member offices?

LIMS is a critical part of the flow of legislative information. It brings in bill information, Floor activity, Member and Committee information, and Executive Communications from the House and Senate and distributes that information to GPO, the Library of Congress, Members, Committees, House Officers, and the public.

Minority Question 7: The Clerk's office is the owner/maintainer of the US Government's sensitive legislative data. Cybersecurity has been a key theme/concern of technology-based organizations for several years now, with an organization's cyber hygiene being a strong indicator of the organization's security posture and readiness.

a. Given that the main mandate of the Clerk's office is to support the Legislative Process and the CAO office is to provide support services, how effectively does the Clerk's office utilize the specialized services provided by the CAO in terms of IT maintenance, specialized cyber security services, and advanced IT planning?

Please see response to Question 5.

b. What coordination occurs between the specialized cyber security organizations of the CAO and the Clerk's office to ensure that the Clerk's office is adequately aware of and protected against internal and external cyber threats?

In addition to regular IT coordination meetings between senior Clerk, CAO, Sergeant-at-Arms and Inspector General staff, LCS staff meet with the CAO Information Security team monthly to discuss security-related information and issues. We are also members of a systems administration distribution list and get updates from CAO Cybersecurity on a regular-basis.

c. Are Clerk IT systems at recommended patch levels and utilizing best practice cyber security standards and frameworks?

Yes, we follow all House Information Security Policies guidelines as well as National Institute of Standards and Technology and Center for Internet Security benchmarks when building and auditing our IT infrastructure. All Clerk servers connected to the House network have security software agents installed on them that provide the CAO Cybersecurity team with real-time visibility into our computer security compliance status. Our systems, computers, and laptops are patched regularly for critical security updates (after testing to ensure system stability).

d. Are the Clerk IT systems actively monitored for attempted internal or external intrusions and is this monitoring effective against the most advanced threats documented in the current cybersecurity threat landscape?

We utilize best-in-class internal and CAO-provided threat protection systems to identify and block malicious activity on Clerk systems and equipment. We monitor our own security systems daily and receive notifications from CAO Cybersecurity about any activity that their applications detect.

e. Given the recent disinformation campaigns targeted at election campaigns by sophisticated adversaries, what advanced mitigations does the clerk deploy to ensure protection and prevent tampering of the Nation's legislative data systems?

The Office of the Clerk employs a range of physical and technical security strategies to protect our legislative systems from threats. Adhering to the House cybersecurity policies is our first line of defense. Implementation of real-time monitoring tools and intrusion protection systems plays a vital role in enhancing our security posture. Also, our staff has been trained to stay operationally vigilant, monitor for any anomalies and provide remediation promptly with each mission critical system. Finally, our contingency plans, which we review and exercise on a regular basis, are in place to mitigate situations if necessary.

f. The last several IG audits have highlighted several strategic cybersecurity concerns, in addition to the tactical findings requiring mitigation. Does the Clerk have a broad cybersecurity strategic plan that is being coordinated with the CAO to ensure consistent and uniform cyber protection across both the CAO and Clerk organizations?

The Clerk IT infrastructure operates under the umbrella of the CAO's House network infrastructure. We adhere to House Information Security Policies which are regularly updated and meet cybersecurity best practices. In addition, we maintain our own IT security layer and monitoring that provide additional protection for the Clerk systems.

To further enhance our IT security posture, we have hired a Senior IT Security Analyst whose primary task is to oversee IT security related activities within the Clerk's Office. This analyst's responsibilities include incorporating security best practices during software development lifecycles and performing regular review of existing systems for potential vulnerabilities.

g. What steps is OHEC taking to proactively reach out and educate Members about best practices and workplace rights?

The Office of House Employment Counsel (OHEC) conducts training for Members and other management, as well as training for non-management staff. Focusing specifically on Member and other management training, OHEC offers training on a variety of employment law topics, including an Overview of the Congressional Accountability Act (CAA), Interview Essentials, the Family and Medical Leave Act, Sexual Harassment, and Litigation Landmines. This training is offered through the Congressional Staff Academy and upon request.

In addition, OHEC is currently working with this Committee to provide Members with Anti-Harassment/Anti-Discrimination training developed for and delivered exclusively to Members as part of the CAA Reform Act and related reform measures.

OHEC also reviews employee handbooks and, in doing so, advises Members and other management on specific policies including EEO, Open-Door, and Anti-Harassment/Anti-Discrimination policies. This process prompts discussions regarding the types of training OHEC offers – both for managers and non-managers. OHEC routinely conducts all-staff training on a variety of topics in both Washington, DC and district offices.

OHEC proactively reaches out to offices in anticipation of the OSHA safety and health and Americans With Disabilities Act accessibility inspections conducted by the Office of Congressional Workplace Rights (OCWR) (formerly the Office of Compliance). OHEC sends a "pre-inspection e-mail" to all House employing offices to inform the appropriate management staff of the inspection process, and

to provide information on the most common safety, health, and accessibility issues. This email includes contact information for the Legislative branch entities responsible for assisting offices in addressing these issues.

As management's legal representative OHEC cannot provide advice to employees regarding their individual workplace rights. However, as part of OHEC's pre-inspection e-mail, it will include a reminder that each office is required to post the Notice of Workplace Rights published by OCWR.

PAUL D. IRVING
SERGEANT AT ARMS

H-124 CAPITOL
(202) 225-2456

Office of the Sergeant at Arms
U.S. House of Representatives
Washington, DC 20515-6634

May 15, 2019

The Honorable Zoe Lofgren
Chairperson
Committee on House Administration
1308 Longworth House Office Building
Washington, D.C. 20515

The Honorable Rodney Davis
Ranking Member
Committee on House Administration
Longworth House Office Building
Washington, D.C. 20515

Re: Response to Questions for the Record

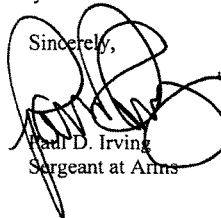Dear Chairperson Lofgren and Ranking Member Davis:

Enclosed are the Office of the Sergeant at Arms responses to the Committee's Questions for the Record.

Please note that the information contained in the USCP related answers were supplied by the Department.

Please feel free to contact me if either you or your staffs should have any additional questions.

Sincerely,

Paul D. Irving
Sergeant at Arms

Questions for the Record
Committee on House Administration
Hearing "House Officer Priorities for 2019 and Beyond"

The Honorable Paul Irving, House Sergeant at Arms

Question 1: What has been the most important factor in the District Security Service Center development of its District Office outreach program?

Feedback from district offices has been the primary factor in the development of our outreach program. Identifying opportunities where outreach is necessary, appropriate and most importantly relevant to district offices has been and will continue to be a primary focus for the District Security Service Center (DSSC). Our outreach efforts include onboarding of new Law Enforcement Coordinators (LECs), educating district staff on the resources available to them, outreach regarding local emergency events and providing useful and timely LEC notices (i.e. reminders about requesting law enforcement support for events prior to recess periods). While we continue to seek relevant topics to expand our outreach efforts, we are fully aware of the daily burden placed on district staff so we seek to provide as much information as possible without unnecessary interruption to their other responsibilities.

Question 2: How many district offices have been impacted by the District Security Service Center program? How many new Members of the 116th Congress and Members' District Offices availed themselves of security awareness briefings as well as the installation of security monitoring systems and Mail Hood devices?

The DSSC has assisted more than 400 district offices with security upgrades to date. Nearly every district office has been impacted when the DSSC security system, mail hood, LEC, training and outreach initiatives are all considered.

Nine freshman Member offices have received Security Awareness Briefings since the start of the 116th Congress. More than 50 freshman Members have received a security system assessment from our vendor and 28 freshman Members have a mail hood in their district.

Question 3: How has the District Security Service Center outreach been received by Members and District Staff?

The DSSC outreach has been well received by Member offices. We have found that many district office staff felt isolated from the support provided on Capitol Hill and the creation of a team dedicated to address their security concerns has been welcomed. In particular, we have received many notes of appreciation from our proactive outreach efforts which involve us contacting district staff when a security related incident occurs near a district office; events such as the active shooter incident in Thousand Oaks, California; the synagogue shooting in Pittsburgh, Pennsylvania; the series of package bombs in and around Austin, Texas; the active shooter incident in Aurora, Illinois; and the recent shooting at a Denver area charter school. The effort is intended to make sure all staff from the office are safe and accounted for and to open a line of communication should the office need any guidance, direction or assistance.

Question 4: Is there currently an established risk/threat assessment analytical protocol established to support the District Security Service Center? Is USCP Intelligence Analysis Division (IAD) a key component supporting the District Security Service Center? Describe how intelligence is collected, assessed and disseminated to appropriate law enforcement partners, as well as Members and Staff?

The DSSC falls within the Police Services Division of the Sergeant at Arms and is dedicated to coordinating District Office security system installation, monitoring and billing support, managing the mail hood program, administering the Law Enforcement Coordinator (LEC) program, conducting outreach, assisting with security training programs and acts as a call center for any security related questions. The District Security Service Center is supported within the greater framework of the joint House Sergeant at Arms (HSAA)/U.S. Capitol Police (USCP) protective services program by serving as an intake point for staff referrals of events and incidents that would benefit from intelligence collection and reporting, and subsequent assignment of law enforcement resources. Congressional staff may visit the District Security Service Center in person, telephone HSAA Police Services directly, or connect online via the HSAA Web EOC portal to initiate HSAA and USCP action. Regardless of the method of intake, the USCP and HSAA follow a systematic and standardized process to collect relevant intelligence, assign appropriate protective resources, and brief cooperating law enforcement partners and stakeholder customers.

At the point of intake, HSAA Police Services staff will ensure that all referrals contain the essential elements of information, and then pass that information to the USCP. At the USCP, the Intelligence Analysis Division (IAD) and the Investigations Division (ID) will collect intelligence based on established intelligence priorities and assess the intelligence for proportionate law enforcement action. The IAD's key role in this process is to draw relevant information from the U.S. Intelligence Community, connect with state and local government fusion centers, and monitor relevant social media and internet sources. The ID's key role is to evaluate the USCP's holdings of known subjects of concern and to connect with Federal, state and local law enforcement officers for relevant information with any nexus to the subject event and participants.

The USCP considers a diverse set of factors when making a risk assessment for a Member of Congress (MOC) event. These factors include, but are not limited to:

- Number of MOCs attending;
- Positions of attending Congressional leadership;
- Persons of interest concerns;
- Organizational/interest group concerns;
- Demonstration/disruption concerns;
- Terrorism threats;
- Crime threats; and
- Position and relevant security threats of other attending dignitaries.

Risk assessment information is collected from a variety of sources including, but not limited to:

- Classified Sources – The U.S. Intelligence Community
- Sensitive But Unclassified Sources – Regional/state fusion centers
- Law Enforcement Sources –LE partners
- Open Sources – News outlets, social media
- Human Sources – MOC staff, interest group spokespersons

Sworn law enforcement personnel from the USCP will share the results of the USCP assessment with HSAA Police Services personnel as well as Federal, state, and local law enforcement partners. The USCP will tailor its final action to the level of concern prompted by the assessment. At the lower end of the spectrum of concern, the USCP will conduct further outreach to the local law enforcement agency of jurisdiction to request an appropriate level and type of police presence at the event. At the higher end of the spectrum of concern, the USCP will plan for more direct involvement by USCP resources, based on the specific circumstances of the individual assessment. Final briefings to Members and staff will be provided by HSAA police services personnel.

Question 5: What can be done further to strengthen the District Office Security Center program moving forward?

As the DSSC continues to mature, we seek to identify additional offerings above and beyond the installation of security systems that will support district staff in improving their overall security posture while harmonizing areas where we overlap with the interests of other partner organizations on the Hill (CAO, USCP).

Some of our focal points over the next year include:

- Onboard New Program Manager Position: The Committee's recent approval of the creation of a DSSC Program Manager position will allow SAA to expand program offerings for district offices and drive greater success of the DSSC program. In particular, this position will be the primary driver of the below listed initiatives.
- Enhance the Law Enforcement Coordinator (LEC) Program: The LEC program serves as a force multiplier for the SAA. While we maintain more than 600 active LECs in our database,

we are exploring ways to better connect with each LEC in the district and increase frequency of two-way dialog with these personnel. Defining a learning path through the CAO's online training system will allow us to standardize baseline training for LECs and the exploration of a periodic, recurring conference call/check-in with LECs will open the door to topics of interest or concern for the LECs.

- Increase Training Offerings: The SAA is exploring opportunities to expand the types of security courses offered to district office staff. To date, we offer Security Awareness Briefings, Mail hood training and active shooter training online. We intend to offer more online training opportunities so that staff can take training at their convenience in a cost-effective manner that has more immediate reach than scheduling face-to-face training in the district. While we initially intend to pursue online self-paced trainings, we are also exploring opportunities for live, remote conferencing style training to increase participation and two-way dialog.

- Expand Knowledge Base of DSSC Team: To continue the development and maturation of the program, we plan to pursue additional training and education opportunities for the DSSC personnel. As the primary call point for district security related questions, increasing the knowledge base of DSSC personnel can serve to ensure district staff are able to obtain quick and accurate answers to their wide-ranging needs.

- Coordinate with CAO, USCP: The SAA has had a longstanding relationship with the CAO and USCP, although our District Security Service Center has existed for just over one year. We continue to work with both entities to ensure aligning interests can be capitalized on and to identify additional converging topics for which we can combine efforts.

Question 6: What is the significance of "Pre-screening" of Members, Staff, and visitors to the Capitol Complex?

The significance of pre-screening individuals coming into the House Office Buildings to enhance the USCP ability to mitigate a threat prior to entering a building. The USCP deploys vapor wake canine units, as well as additional officers as needed, around the campus to address any potential threat before it enters a building.

Question 7: What are the risks of not having 100% of the Members, Staff, visitors and vehicles being fully screened prior to entering the Capitol Complex?

If individuals are not screened, they could introduce dangerous items into the building, such as firearms, explosives, and knives of prohibited length.

Staff and visitors are screened when coming into the buildings from any of the external entry points. Presently, staff entering the building from the Rayburn or Cannon garage are not screened. Screening from the Rayburn and Cannon garages will begin August 5, 2019.

With regard to vehicles, Members and staff are only allowed to park in the garages and most lots. The USCP conducts vehicle checks and patrols the garages and lots.

Question 8: How will the establishment of a North and South Capitol Screening Kiosk solidify the security of the Capitol? Will the development of these screening Kiosks allow the USCP to better align its sworn personnel resources protecting the Capitol Complex?

The establishment of a South Capitol Screening Kiosk will solidify the security of the Capitol by removing the screening of staff and guests out of the Capitol building. In addition, the Kiosk, as currently envisioned, will have certain security features such as blast protection which will mitigate any damage resulting from an explosive device. In addition, the Kiosk will be equipped with a portal scanner similar to those currently deployed around the House Chamber. This will detect any non-metallic hazards, before it enters the Capitol Building.

The USCP will still need to staff the screening in the Kiosk. Any realignment of posting will be determined in the future based on the impacts of the Kiosk.

Question 9: The Capitol Complex Garage Security Enhancement Project is in its final phases. How will this modified infrastructure harden the garage complex security and improve Members and Staff movement between the House buildings and Capitol?

The Office of the Sergeant at Arms continues to work with the Committee, the Architect of the Capitol and the Capitol Police to implement screening in the House garages. Garage security modifications will bring the Capitol complex closer to 100% screening by adding USCP officers and screening equipment at all accessible entrances from the Rayburn and Cannon garages. Once implemented, staff parking in the Rayburn and Cannon garages will be screened prior to entering the House Office Buildings. This will ensure the same level of screening whether using the pedestrian street entrances, the garage entrances to all House (and Senate) Office Buildings or the pedestrian entrances to the Capitol. The addition of the garage screening will harmonize our security posture with the Senate Office Buildings. This improvement should eventually allow Members and staff to move from the House Office Buildings to the Capitol without additional interior magnetometer screening in the Rayburn and Cannon tunnels since House Office Building occupants have all passed through screened entrances.

Question 10: Is the USCP prepared to physically cover the expansion of garage and new screening positions for the final phases with its current resource constraints?

Yes. The garage security initiative is a multi-year project, and the USCP has been hiring additional FTE for this initiative since 2018. The USCP has hired, trained and graduated all of the necessary 52 new sworn officers necessary to implement the House Garage Security Initiative. The final portion of these new sworn officers will complete their Police Training Officer (PTO) program in late May 2019, after which all 52 sworn officers will be ready for the full implementation of the Initiative

Question 11: The USCP-OIG has outlined several challenges facing the USCP moving into the future. Has the USCP completed a new strategic plan to improve its recruitment, development, and retention of a sworn and civilian diverse workforce?

The USCP Strategic Plan for Fiscal Years 2020-2024 is currently under development. The new strategic plan will highlight mission and mission support goals and strategies that will provide the roadmap into the future. The success of the Department's mission relies upon a highly engaged, highly skilled and diverse workforce. The new plan will define new and evolving law enforcement strategies to strengthen the USCP's mission; those that further the overall global protective approach to security and protection, leverage specialized units and functions in the Department in new ways; and expand in a more significant way the cyber and technological tools needed in the investigation of threats. Additionally, the new plan will address and emphasize the USCP's human capital and the human capital lifecycle. The strategic goals contained in the USCP Strategic Plan will be the foundation for informing the USCP Human Capital Strategic Plan, which is also under development.

The Human Capital Strategic Plan will outline specific goals, objectives and critical success factors supporting recruitment, retention, development, and rewards incorporating human capital and diversity and inclusion best practices across both law enforcement and Federal communities. Finally, diversity and inclusion strategies, action plans, and measures will be outlined to ensure the USCP workforce reflects the diversity across our nation. USCP priorities and measures of success will be clearly defined and communicated across the Department to ensure the visibility and support critical to increasing diversity, inclusion, and equity while increasing employee engagement and commitment to USCP Human Capital goals.

Question 12: The collection, evaluation, and dissemination of intelligence is important for the protection of Members, Staff, visitors, as well as District Offices. What is the USCP plan of action to modernize its intelligence processes and cadre?

The USCP maintains a professional staff of intelligence analysts, sworn field agents, and technical support personnel well trained in modern techniques and methods that support the Department's mission to protect Members of Congress, Congressional staff, and visitors to the Capitol Complex. The USCP maintains full IT connectivity to classified channels of the U.S. Intelligence Community. Furthermore, the USCP sustains full-time liaison positions with 9 Federal partner task forces/organizations to facilitate the exchange of intelligence and law enforcement information with a nexus to Congressional protection. The USCP coordinates on a daily level with the Federal Bureau of Investigation, the U.S. Secret Service, and the Department of Homeland Security on intelligence related matters.

In 2018, the Investigations Division (ID) opened 5,206 protective intelligence/threat management cases and 640 law enforcement coordination cases for off-campus Member of Congress (MOC) events. In 2018, the IAD prepared and delivered 3,533 intelligence products that were utilized to make significant operational decisions and drive the assignment of law enforcement resources for protective services.

In 2018, the USCP pursued a number of initiatives to enhance and expand upon intelligence collection and analysis. The ID was expanded by the reallocation of 15 sworn personnel from elsewhere in the Department to keep pace with increasing numbers of protective intelligence case investigations. The IAD completed training for the implementation of newly acquired computer software that enhances the USCP's ability to proactively search for, and respond to, internet/online threat streams. Finally, the USCP created an additional dedicated liaison position on a Federal cyber-crime task force to increase its existing ability to detect and investigate cyber-crime that targets MOCs.

Currently, the USCP is pursuing a number of new investments in its overall intelligence program. First, the USCP is evaluating the addition of new full-time equivalents (FTEs) to the IAD to expand its hours of operation, strengthen supervision and management, and enable proactive searches of intelligence sources at a deeper and more detailed level than can be pursued at the current staffing level. The USCP is also evaluating the assignment of a dedicated liaison position to coordinate protective intelligence concerns occurring outside the continental United States (OCONUS). Finally, the USCP is evaluating the addition of further new technology and methods to enhance the collection and assessment of internet/online threat streams.

Question 13: The OIG recommended the elevation of USCP's Intelligence Analysis Division to a Bureau or Office level in a previous OIG report? What progress has the USCP made to transform the intelligence structure? What is the impact positive or negative of the USCP transforming the intelligence structure?

In 2016, the OIG completed an audit report of the USCP Intelligence Analysis Section and issued 6 recommendations as an outcome of that report. The Department has successfully closed all 6 of those recommendations. In 2018, the OIG completed a resolution analysis of the previous report and issued 5 recommendations as an outcome of that report. The Department has successfully closed all 5 of those recommendations. The OIG has not issued any formal recommendation in either of those reports, or any other report, in which the OIG recommended a reorganization.

The Department has been planning a reorganization since 2015 and the Department's reorganization plan was implemented on January 1, 2018, following the approval by the Department's oversight authorities, and included a change to elevate the Intelligence Analysis Section, previously organized under the Investigations Division to become the Intelligence Analysis Division, now organized under the Protective Services Bureau. This option was taken as the best combination of increasing the stature of the USCP intelligence analysis function, along with maintaining the necessary close connectivity to the ever-increasing protective intelligence investigations and law enforcement coordination operations undertaken by the Investigations Division.

The USCP continues to pursue initiatives that will further transform the Intelligence Analysis Division. Of particular note is a proposal currently being evaluated within the Department's established business process for new investment to increase the staffing level of the IAD (see response to Question 12) to expand its hours of operation, strengthen supervision and management, and enable proactive searches of intelligence sources at a deeper and more detailed level than can be pursued at the current staffing level.

Since 2016, the Intelligence Analysis Division has undergone a number of internal changes, including the adoption of a standardized intelligence priorities framework, the revision of many operating procedures, the refocusing of its intelligence products, the adoption of new technologies and methods of collection and analysis, and the establishment of new partnerships with other agencies. These progressive transformations have enhanced the USCP's ability as a whole to protect Members of Congress both within and beyond the U.S. Capitol Grounds.

Question 14: Does USCP current intelligence structure efficiently and effectively support the SSA's District Security Service Center needs? Is there appropriate integration to address Members and District Offices needs with vetted and validated intelligence?

Please see the response to Question 4 of this document for a detailed description of how the current USCP intelligence structure is aligned to the House Sergeant at Arms (HSAA) District Security Service Center. HSAA Police Services staff interact and coordinate on a daily basis with USCP personnel from the Protective Services Bureau (PSB) to address the security needs of Members of Congress (MOC). Working in close cooperation with the HSAA, the USCP believes that the current processes and procedures support the needs of the District Security Service Center and the overall effort to provide effective and efficient protective services to Members outside the U.S. Capitol Grounds.

Question 15: What is the status of the USCP and FOP Collective Bargaining Agreement (CBA) which was last ratified in June 2010? When was the last time the USCP Executive Management and FOP formally met to discuss the development and ratification of a new CBA?

The development of a new CBA is on hold pending the resolution of several ongoing court cases. As per the provision in the contract, the USCP and FOP/USCP Labor Committee will continue to operate under the existing contract until such time a new contract is finalized. The delay of a new CBA has not impacted the union and USCP management relationship or the implementation of new and improved programs and policies. To that end, USCP management and the FOP will continue their regularly scheduled biweekly meetings and work through matters on a case-by-case basis, as needed.

Question 16: What is the USCP doing to update its Disciplinary Policy?

Over the last several years the Department has been working to update and implement a discipline process that captures the current practice. The Department has drafted a policy that does such, and when published, will apply to all USCP employees, to include employees within the collective bargaining units. The USCP intends to issue the draft policy as Interim Guidance, which will articulate the revised discipline process and ensure transparency for the employees, until such time as the unresolved issues can be addressed.

Question 17: How do the new employee standards integrate with USCP Disciplinary Policy?

The USCP Employment Suitability Standards (Standards) for new employees were revised and approved by the Capitol Police Board on September 26, 2018. These new Standards were designed to identify the best qualified applicants by increasing the objectivity, clarity and consistency of the minimum requirements to become a police officer, hazardous material technician or civilian with the Department. The previous USCP hiring standards were issued in 1997, and were considered dated for the recruitment and hiring of the best qualified personnel to fill the USCP's law enforcement and civilian positions.

Separate from the Standards is the Department's disciplinary process. The disciplinary process addresses behavior post-employment, with the employee's conduct and performance being measured against the Department's policies and procedures. However, by ensuring that the USCP is hiring the best qualified applicants, the Department believes that the individuals hired under the new Standards will have the depth and breadth of knowledge and skills to successfully apply the Department's established policies and procedures in conformance with the respective expectations, thereby having a direct effect on the frequency of the application of discipline.

Question 18: What is the USCP doing to update outdated corporate policy and guidelines?

The USCP Office of Policy and Management Systems (OPOL) is responsible for the overall management of the Department's Directives and Standard Operating Procedures (SOPs). The creation, revision, and rescission process for Directives and SOPs is continuous and can be initiated at any time by any USCP subject matter expert with chain of command review and approval. Per Department policy, at a minimum, OPOL facilitates an annual review of the Directives and SOPs with the respective USCP Bureaus/Offices to ensure those policies are both current and applicable. Currently there are 37 Directives and 87 SOPs in the revision process.

Since January 1, 2013, 98 new SOPs adopted, 367 old SOPs have been revised, 59 new directives have been adopted, and 67 old directives have been revised.

Accordingly, the Department will continue to maintain its review and issuance posture of Directives and SOPs to ensure law enforcement and/or other specialized best practices are included in USCP policy and practice, and that all Directives and SOPs are accurate for the respective Department elements' area(s) of responsibility.

Question 19: What is the USCP strategic plan to recruit and retain a diverse workforce?

A new USCP Human Capital Strategic Plan is currently expected to be completed at the end of calendar year 2019. It will outline very specific goals and strategies with action plans and metrics that address the recruitment and retention of a diverse workforce. Developing a hiring strategy to recruit a diverse workforce, one that reflects our nation, is a high priority. Increasing the diversity within the USCP workforce, at all levels, will allow for greater employee productivity, unity, and engagement within the Department. The USCP will continue to look at best practices in law enforcement organizations as well as across all sectors, to ensure success in gaining the benefits of increased diversity and inclusion. More specifically, as an organization, the USCP is reviewing the implementation of potential practices such as:

- review and craft job postings that will attract a more diverse workforce
- update and offer new policies that appeal and support diverse candidates
- implement recruiting tools based upon compatible personality traits, motivations, and skills that do not differ across minority groups
- implement sourcing methods (third party websites etc.) that contain more diverse candidate pipelines
- "seed" pipelines with more diverse candidates (Harvard Business Review noted research "two in the pool effect" represents a promising method for overcoming unconscious biases and increasing diversity)
- increase professional development and training
- improve the management and implementation of reasonable accommodations

Specific diversity and inclusion strategies and actions will be highlighted and emphasized as the USCP develops its overarching Strategic Plan and the resulting Human Capital goals and strategies.

Question 20: The USCP has noted it has difficulty training its personnel without allocating over-time. What is the direct impact of minimal training and career development of USCP personnel?

For the Department to meet its basic operational mission requirements, there is a delta of nearly 200 sworn personnel shortage to mission requirements, which significantly impacts the USCP's ability for officers to be off post to train beyond mandatory life-safety training requirements. Therefore, the Department requests 24,000 hours a year for overtime to be specifically utilized for in-service training for sworn personnel in its annual budget request. However, in the interim, the Department will continue to apply available resources from the Training Services Bureau to deliver the most critical life-safety, use of force, and legal update training to all sworn personnel. In FY 2021, the Department will be reviewing this level of request to account for the increased sworn staffing levels recently hired to address the four enhanced security initiatives.

While the Department intends to further develop its succession planning process as well as other types of training and career development opportunities, it would be difficult for the USCP to holistically implement, rather than case-by-case, such programs with the current mission

requirements and sworn staffing delta as stated above. Nevertheless, the Department will be including these important and necessary developmental processes in both the USCP Strategic Plan for Fiscal Years 2020-2024 and the Human Capital Strategic Plan, which will include diversity, inclusion and equity.

Question 21: What progress has USCP made to enhance the capabilities of the Office of Information Systems protect USCP IT systems?

The USCP Office of Information Systems (OIS) protects the Information Technology (IT) infrastructure and endpoints as defined by the goals presented in the USCP IT Strategic Plan, Fiscal Year (FY) Operating Plans, and system enhancements through the Force Development Business Process. The OIS partners with other Legislative Branch Offices (LBO) through both the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) Councils and continually collaborates on security issues within the Legislative Branch Cyber Threat Intelligence Working Group (LBCTIWG) and the SOC-to-SOC Working Group. Monthly meetings are held with the USCP Executive Team (COP, COO, CAO, OGC) to discuss current status of ongoing projects, upcoming initiatives, and current risks and issues.

The USCP OIS Information Security Division's (ISD) mission is to "...implement and provide a secure enterprise solution which embraces the Department's mission and utilizes technology to operate securely and efficiently while reducing operational risk." The ISD has successfully become a business integrator, has increased transparency, enhanced visibility, and ensured business continuity. OIS has defined mission objectives with high level milestones to reduce risks and further the protection from various cyber threats at an enterprise level.

Some notable successes supporting the maturity of one or more of the cyber domains are listed below:

- Implemented certificate-based authentication on wireless mobile devices and finalizing other multi-factor authentication initiatives.
- Implemented a new enterprise Security Incident and Event Management (SIEM) solution.
- Implemented Senate threat feeds into our SIEM.
- Implemented the advanced Security Awareness Training solution utilizing a two-phase approach to increase training and user awareness.
- Established the vulnerability management program using Qualys for advanced vulnerability assessments and continuous monitoring.
- Enhanced two-factor authentication with an advanced solution and use of soft tokens.
- Completed full integration of the Security Orchestration Analysis and Response (SOAR) utilizing Swimlane for automation of security events to lessen time spent on false positive, faster response times for actionable alerts, and a consistent method for all alerts.
- Partnered with MindPoint to structure and mature the Assessment and Authorization (A&A) program and establishing four Authority to Operate (ATO) certifications and supporting documents.

- Implemented Qmulos in support of the A&A program; providing security control status, POAMs, and document repository.

ISD is achieving its annual targets and moving closer to achieving the strategic goals and objectives outlined in the IT Strategic Plan. A great deal of progress has been made in securing the USCP environment combined with overall user awareness and training.

Question 22: What bench marks have been achieved per OIS's outlined Strategic Plan FY 2017-2021?

The USCP IT Strategic Plan 2017 - 2021 is reviewed annually to ensure it remains current and aligned with USCP mission priorities. Near the end of each fiscal year, the OIS conducts an annual review to highlight accomplishments from the previous year, identifies new opportunities and challenges, and develops streamlined governance and service delivery processes to become more efficient and effective. During this period, OIS develops an operational plan outlining priorities (projects and initiatives) for the upcoming fiscal year based upon organizational priorities, funding, commitments, and essential operations and maintenance of USCP IT infrastructure.

The OIS has been very successful in delivering products and services as defined in the annual operational plans. Each year, as projects are delivered and services enhanced, the OIS is closer to achieving the strategic goals outlined in the IT Strategic Plan. As new mission priorities are introduced, the OIS remains nimble and adjusts resources to focus on new or unplanned requirements. Strong program and project management with OIS-wide quarterly reviews, ensures projects stay on track and/or risk mitigation practices are put into place. The strong governance process allows for transparent and sound decision making and critical adjustments without compromising day-to-day operations. Across the board, OIS is consistently improving and meeting both strategic and annual commitments and planned targets.

OIS will begin the development of the new IT strategic plan upon the completion of the Department Strategic Plan to ensure the strategic goals for information and technology both align, support and lead the Department into a more modern, premier, technology driven law enforcement organization.

Key accomplishments include:

- Joint Emergency Mass Notification System (JEMNS) - USCP hosts this LBO-shared emergency notification solution
- Web EOC – implemented an emergency and operations incident management tool supporting the Command and Coordination Bureau in command and control operations
- Skype for Business – an enterprise solution that is federated with the LBOs for enhanced communications and collaboration
- Remote access solution deployed - Citrix
- Radio System (infrastructure) Lifecycle Refresh
- Radio Systems Updated (Congressional Leadership)

- MPD data integration completed • iPhones and AirWatch – implemented a USCP mobile application "store" with security enabled mobile application vetting (moved away from once standard BlackBerry devices)
- VTC upgrades
- Radio – Red One Back-Up
- Firing Range Tracking System (FRTS)
- Soft Tokens – supports remote access to USCP employees without the need for a separate physical device
- Modernized security incident alerts
- Implemented and operate under a new Cyber Maturity Model
- OIS-wide Process Improvement: new and improved processes have proven to add greater efficiency, role clarity, and increased collaboration, ultimately improving our service delivery

Question 23: The Committee's oversight plan for the 116th Congress notes that we will review staff ID standards. Are the IDs provided to staff appropriate as a form of security identification?

The staff identification badges do act as a sufficient form of security identification for an open campus.

The ID's are printed on HID RF-Programable 125KHZ cards. These cards have encryption keys for purposes of proximity access.

The badge is provided to staff members and paid interns only after the appropriate I-9 and payroll paperwork has been filed with the Office of the Chief Administrative Officer, the Architect of the Capitol or other supporting agencies. In addition, all staff and all interns must present a form of government identification to the SAA ID office prior being provided the badge. Acceptable government identification includes a US passport, State issued drivers license or non-operators ID, and US Military ID. For individuals who may not be United States Citizens, they must produce a valid passport or a USCIS issued Green Card.

Contractors are required to produce to the ID office acceptable government identification, as outlined above, and a certification of their completed background check must be approved on their application form.

As the House Office Buildings are open to the public, the IDs are color coded. The codes identify those staff who are permitted access to the buildings at any time (currently a red badge) and those staff and interns who may only be in the buildings during business hours (currently a yellow badge). The ID also contains the office for which the individual works in the event that there is a situation where the individual is found to be in space where the individual is not authorized.

Questions for the Record from the House Administration Minority

Question 1: You are planning to spend $3 million dollars to replace annunciators in offices, the new units will cost $1,500 each. Are we investing in dated technology? What market research was done to see if a more cost-efficient solution exists?

The annunciator replacement project, also known as the Joint Audible Warning System (JAWS) will replace an outdated, non-secure emergency notification system with a digital solution that provides greater clarity and audibility of message, encryption for security, and enhanced resilience to ensure emergency messages reach all parts of the Capitol, CVC, and House Office Buildings when required. The annunciators serve as the only effective way to ensure every office and area of the Capitol and House Office Buildings receives necessary safety information.

In 2017, HSAA, SSAA, AOC, and USCP began the project to replace the aging annunciator system by conducting market research that examined what products or solutions may fit a base requirement of in-office verbal emergency notification. The market research effort was led by the subject matter experts within the USCP radio unit who know the radio transmission industry and supported the House, Senate, and AOC project team in the development of the initial requirements. The initial requirements framed the Request for Information that was put out to industry on FedBizOpps (www.fbo.gov and operated by the General Services Administration). The Request for Information allowed companies in the public address/emergency notification industry to provide products, concepts, and solutions that could possibly meet a wide set of requirements set by the Legislative Branch.

At the same time, USCP evaluated the option of using existing radio or communications infrastructure to support this project. Due to security vulnerabilities that would be created using existing USCP infrastructure to meet this requirement, this concept was removed from possible options.

Upon review of the provided responses and obtaining a better understanding of the current state of the marketplace, the project requirements were further refined. A Request for Proposals was released in December 2018. Those proposals are currently under evaluation by the project team.

Question 2: In recent years a top priority of your office has been enhancing physical security in district offices and at district events. Can you highlight some of the specific services your office provides in that effort?

Over the past 19 months the Sergeant at Arms (SAA) has worked with more than 400 district offices to upgrade or add security systems in their offices. In addition to allowing Member offices access to our national contract, the SAA funds the installation of one base system per Member. Our standard system includes an intrusion detection system which can serve to notify staff and law enforcement in the event of a break-in outside of business hours, a duress system which allows staff to discreetly notify law enforcement should a threatening visitor cause a disturbance and a video intercom system which allows staff to speak with visitors before allowing them into the office. In addition to funding the installation of an alarm system, the SAA

14

covers the cost of monthly monitoring fees for all district offices thus reducing MRA expenses for security services.

The SAA Police Services Division also offers law enforcement coordination services for Member events in their district. Upon notification of a district town hall or other event, the SAA with the assistance of the U.S. Capitol Police (USCP) will contact local law enforcement agencies to request security support for the event. USCP also conducts an open source check to identify any known or potential protests related to the event so that the Member office and local law enforcement can be made aware. Since January of last year, SAA has coordinated support for more than 600 such district events.

The SAA also maintains a Law Enforcement Coordinator (LEC) program. This initiative seeks to identify at least one staff Member in the district who serves as the primary liaison between the office, local law enforcement, the SAA and USCP. We view this program as a force multiplier, expanding the overall security support provided by our office. Our service center conducts regular outreach and awareness messaging to these personnel and we continue to expand this program today. The SAA also provides mail hoods to allow for safe handling of incoming office mail and training to district offices to increase security awareness amongst staff.

Question 3: Since completing this last Congressional transition what is the status of outreach to the new Members and their participation in the standard security system package for their district office?

The District Security Service Center (DSSC) has successfully reached out to all freshman Member offices to educate them about the DSSC and the security services and support available through the SAA. We are happy to report that many Members obtained an office previously secured by their predecessor which reduces the overall need for security upgrades. Although leases continue to be signed, the SAA has completed security upgrades at more than 30 district offices for freshman Members. At this time, only four freshman Members have not yet made a decision to proceed with SAA standard security system package although none have formally declined.

Question 4: What are your thoughts on whether we should have a dedicated coordinating office to make sure events that Members hold off the hill have adequate security?

Based on the feedback we have received to date, the current structure provided by the SAA appears to provide adequate support for Member events. SAA Police Services Division offers security assessments and law enforcement coordination for Member events on and off Capitol Grounds. Upon notification of an event, the SAA with the assistance of the USCP will contact local law enforcement agencies to request security support for the event. USCP, with information collected from staff, local law enforcement and open source checks, completes a security assessment. This assessment attempts to identify any known or potential protests related to the event and any known persons of interest in the area of the event. Since January of last year, SAA has coordinated support for more than 600 such events.

Question 5: Many government agencies have adopted a badging process to enable utilization of a trusted workforce with specific privileges in terms of ensuring trust, easing access, and promoting efficiency.

The implementation of a trusted agent badge would require the creation of a specific process to allow for the vetting of staff backgrounds. Currently, it is up to each Member to determine what level of background investigation is conducted for each employee. This could delay the hiring and badging process if applied to new employees. However, a program such as this will shortly have little impact on the ability of staff to traverse the campus. Staff will still be required to be screened at the entrance to the buildings. Screening at the entrance to the buildings is necessary due to items, such as firearms, that are prohibited. With the implementation of garage security, the House Office Buildings will be brought within the secure perimeter and upon the harmonization of the prohibited items list between the Capitol and the House Office Buildings, staff will be allowed to traverse throughout the Capitol complex without going through screening, making all staff, in a sense, trusted agents.

Question 6: What steps are the CAO and SAA offices taking together to improve identity management and governance throughout the House?

The CAO has implemented the Identity Hub, which streamlines the processes for entering, updating, and accessing employee identity-related information. The Identity Hub improves controls for managing access to various House resources such as the House network, financial systems, and privileged accounts. Once complete, the House will have one reliable system of record that will improve data security and the efficiency of House business processes.

The House Sergeant at Arms, working with the House CAO, has initiated the use of a unified Identity Hub to share information between the two House Officers. We are currently piloting a paperless submission program for ID Badge requests, that will be made available House-wide in the coming months. This new process will enhance security around ID Badge distribution through the use of an automated workflow to ensure we are receiving badge requests only from the appropriate personnel. As the collaboration between the SAA and CAO continues additional data sharing processes will be implemented, to include automatically updating the status of House personnel in SAA and CAO systems as they are on-boarded and off-boarded.

Question 7: What steps are the SAA taking to improve badging, authenticating, identifying and vetting of individuals with access to the Capitol Hill complex?

The badge is provided to staff members and paid interns only after the appropriate I-9 and payroll paperwork has been filed with the Office of the Chief Administrative Officer, the Architect of the Capitol or other supporting agencies. In addition, all staff and all interns must present a form of government identification to the SAA ID office prior being provided the badge. Acceptable government identification includes a US passport, State issued drivers license or non-operators ID, and US Military ID. For individuals who may not be United States Citizens, they must produce a valid passport or a USCIS issued Green Card.

The House Sergeant at Arms, working with the House CAO, has initiated the use of a unified Identity Hub which shares information between the two House Officers. We are currently piloting a paperless submission program that we will roll out House-wide in the coming months further ensuring we are only receiving paperwork from approved senders. Additionally, HSAA Staff recently reviewed hardware solutions that would act as an additional check to ensure that Identification (Passports, State Drivers Licenses, Green Cards) are valid.

Philip G. Kiko
Chief Administrative Officer

**Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515–6860**

HB–28, The Capitol

May 15, 2019

The Honorable Zoe Lofgren
Chairperson
Committee on House Administration
1309 Longworth House Office Building
Washington, D.C. 20515
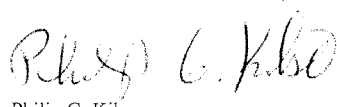
Dear Chairperson Lofgren:

Attached are the Chief Administrative Officer's written responses to the Committee on House Administration's questions for the record following the April 9, 2019, hearing, "House Officer Priorities for 2019 and Beyond."

Additionally, per your request, a summary of the Chief Administrative Officer's diversity hiring practices is attached.

Please contact me or Anne Binsted at 202-225-5555 if you or your staff have questions regarding the written responses.

Sincerely,

Philip G. Kiko
Chief Administrative Officer

cc: The Honorable Rodney Davis
    Ranking Member

101

Philip G. Kiko
Chief Administrative Officer
U.S. House of Representatives

Questions for the Record from the House Administration Majority

Question 1: CAO plays an integral role in transition operations between Congresses. What challenges did the office face transitioning into the 116th Congress?

Answer: There were a number of factors that made this transition more challenging than years past. However, the transition was a success thanks in no small part to the overtime hours worked by dedicated CAO staff and the close collaboration with the Committee and other House partners. Highlighted below are a few challenges specific to the transition to the 116th Congress. Additionally, attached is an infographic providing an overview of CAO efforts to support the transition.

- **Historic class size:** The 116th transition marked the second largest transition in CAO history. Providing administrative, technical, financial and logistical support to this tremendous number of new, departing, and returning Members and staff was challenging for our finite number of staff. While we had some staff augmentation contracts in place, the volume of work was still impressive.
- **Leadership changes:** The last Committee and Leadership moves precipitated by a flip occurred eight years ago. Therefore, the guidance documents and processes needed to be refreshed and executed in a very short timeframe while new, departing, and returning Member activities were simultaneously underway. The CAO's staff worked collaboratively and adjusted quickly to last-minute schedule changes and office requests.
- **Number of Contested Races:** In addition to the large class of new Members, there were a large number of contested races that remained uncertain for a number of weeks. When election results are uncertain, CAO teams have to delay office setup actions for the potential new Members involved in the race. Similarly, they have to delay office shutdown actions for the potential departing Members. These delays ultimately shrink the timeline to accomplish the tasks necessary for new Member offices to be operational at the start of the new Congress.
- **Government Shutdown:** The government shutdown presented challenges for the transition in that our GSA partners were initially furloughed at the beginning of the shutdown in late December. After CAO leadership engaged GSA leadership about the critical support needs, GSA Congressional Support Representatives resumed their activities after a one-day lapse in service.

Question 2: How often does CAO review and revise its procurement guidelines?

Answer: The CAO continuously reviews and evaluates the House procurement guidelines to identify opportunities to improve the efficiency and effectiveness of the House acquisitions processes. The last revision of the Guidelines for Procurement of Goods and Services for the House of Representatives was adopted by the Committee March 18, 2010. In February 2017, the CAO's Office of Acquisitions Management submitted suggested revisions to the procurement guidelines to the Committee for its consideration. It is the CAO's understanding that those revisions are still under review.

Question 3: How will CAO measure success with the Customer Experience Center?
Answer: The CAO's vision is, "to be an essential resource for every Member of the People's House through outstanding customer experiences delivered by exceptional employees." In its Strategic Plan, the CAO identified customer goals, including increasing customer satisfaction through improved service delivery. To help fulfill its vision and achieve its customer goals, the CAO created the Customer Experience Center (CEC).

The CEC is comprised of existing, modified, and new services focused entirely on serving Member, committee, and leadership offices versus the organization itself. For example, it combined its graphics and photography shops and added videography capabilities to what is now House Creative Services – a one-stop-shop for offices' digital needs with a modernized online platform and enhances product offerings. Its new Congressional Staff Academy offers professional development courses specifically requested by House offices as well as required technical training courses. The CEC also includes new Customer Advocates dedicated to helping their assigned Member offices navigate and access services provided by the entire organization. Advocates also gather and relay customer feedback to CAO service providers so that services can improve and evolve as needed to best meet customer needs.

The best measure of the CEC's success will be whether the use of CAO services increase and whether customer satisfaction with its services – old and new – improves. The CAO is incrementally increasing the use of customer satisfaction surveys, which are currently being deployed to recipients of over 30 transactional services provided by the CAO. As its survey capabilities mature, it will survey satisfaction with consultative services and use the baselines of each to measure varying levels of customer satisfaction.

The CAO will also measure the success of the CEC by periodically gauging its brand awareness and ease of access as reported by its customers. To improve its brand awareness, its Communications and Marketing team has been tasked with ensuring communications from every service division within the CAO are accurate, easily understood by our customers, and consistent. CAO Communications and Marketing is also working to ensure the CAO is communicating with modern methodology that our customers expect in the 21st century.

The CAO wants Members to rely on its services by choice and measuring the number of offices the choose to use CAO services and their satisfaction will determine if the CEC is successful.

Question 4: Responding to district office concerns presents unique challenges. How does CAO adapt to that?

Answer: From technology support, to staff training, to financial services, the CAO offers a broad spectrum of services to House employees. Though the services provided by the CAO are generally available to both D.C. and district offices, familiarizing district office staff with the services and ensuring they have equal access to them remotely can be challenging.

To address this challenge, the CAO's Customer Experience Center (CEC) has partnered with its service teams to improve district office access to and awareness of CAO service offerings. For example, the CAO's Office of Finance collaborated with the CEC's Congressional Staff Academy to offer required financial training courses online. The Office of Employee Assistance has also partnered with the Congressional Staff Academy and House Information Resources to provide district staff with remote access to their live training sessions on personal and professional wellbeing. The Office of Employee Assistance also regularly consults with District Directors about performance matters and training opportunities to support staff development.

The newly formed House Wellness Center is recording their training offerings and will make them available on their website. Once those training offerings are posted, D.C. and district-based staff can log into the site to view them at any time.

The CAO's technology support for district offices has also improved. In addition to facilitating new technology requirements that improve office connectivity and operational capabilities, such as broadband and VoIP, the CAO has worked to improve internet connections for district offices on the West Coast.

The CAO's asset management efforts are complicated by the geographic dispersion of district offices. Not having district office inventories within arm's reach of the CAO's asset management team requires great reliance on district office staff and others to tag new assets, conduct physical inventories, and provide confirmation/documentation for equipment disposals and/or hard drive destruction. To address the challenges specific to district office inventories, the CAO has increased proactive and follow-up communications between its asset management team and GSA's Congressional Support Representatives to ensure necessary inventory processes are being executed. In fact, the CAO utilized SharePoint collaboration software for the first time during the transition to the 116th Congress to automate and expedite communications with GSA.

To support district office transition activities, the CAO looked for opportunities to clarify and add new tasks that would assist their transition efforts. For example, the CAO added new streamlined forms, supplemental materials, and district-specific tasks to the departing Member website. For the returning Member website, a new district office task-tracking section was added that focused on district office lease renewal requirements and other critical district move-in/move-out tasks. District office survey outreach has also been more

robust this year compared to past transitions with the addition of Customer Advocates. Leveraging their regular communications with offices, they have been able to gather valuable feedback that is being incorporated into our holistic transition after-action review.

The CAO's newly formed Office of Employee Assistance works to ensure that district office staff have equal access to its free legal services and regularly utilizes a range of electronic, telephonic, and video technologies to communicate with staff. When appropriate, attorneys also travel to district offices to assist employees. Similarly, at the direction of the Committee, the CAO has worked to ensure that the required, in-person Workplace Rights and Responsibilities Training is hosted in locations geographically convenient to Members' district offices.

To promote greater awareness of all of the CAO service offerings and to learn more about district offices needs firsthand, the Customer Advocates have been visiting district offices across the country. Since the program started, Customer Advocates have visited district office staff from over 60 congressional offices – half of which are freshman offices of the 116th Congress. The CEC also participates in the district office outreach initiative to identify opportunities to improve services provided to district offices.

Question 5: In your testimony to the Legislative Branch Appropriations Subcommittee you mention $2 million in savings from district office upgrades. Can you expand on that?

Answer: The savings were directly related to the migration of all Member flagship or primary district offices from data routing technology called Multiprotocol Label Switching (MPLS) to Broadband. The cost to provide MPLS data connectivity to a district office located in the continental U.S. was $542.00 per month, per office. The MPLS cost for all flagship or primary district offices totaled $2,829,240 annually. By comparison, broadband costs $147.00 per month, per office, which totals $767,340.00 annually and yield a savings of approximately $2 million annually.

Question 6: CAO currently employs 719 authorized fulltime employees with 75 vacancies and nearly 300 contractors working across eight CAO business units. What is the internal process the CAO uses to evaluate whether to use an employee or a contractor for a given project. Are you satisfied with the management of the contractors?

Answer: The CAO's Human Resources' workforce planning team works with all departments to analyze the organization's current and emerging workforce requirements and ensure the organization has the appropriate employees and talent on board to meet its operational and strategic needs. The workforce planning processes identify gaps and situations where utilizing contract support is a value-added strategy.

The following criteria is considered to determine whether to utilize an employee or contractor to work on any given project, program, or activity:
- The nature of the work (the CAO has a wide breadth of services with various operational demands).
- The duration of the work to be completed (short-term project, long-term service delivery, etc.).

- The timeliness of the completion of the work (an immediate requirement or a future project/activity).
- The required skill set needed to accomplish the work (due to the breadth services across the business units, the skillsets across the organization vary greatly).
- The impacted business unit's available resources (both personnel and non-personnel resources).

As explained in the CAO's response to question 9 below pertaining to Contracting Officer's Representatives (CORs), the CAO has improved its COR training curriculum to better assist CORs in performing their required duties. Contractor management has improved as a result of the enhanced training, and the CAO is currently satisfied with its management of contractors.

Question 7: During transitions, there is a spike in contactor support. What is the average number of contractors retained to support transitions?

Answer: During transition years, there is an influx of contractors onboarded between October and December to support transition efforts. The CAO onboarded 324 contractors in 2016 and 372 in 2018 between October and December.

Question 8: The Committee understands the CAO uses Contracting Office Representatives (CORs) to manage contracts. What is the total number of CORs and how many contracts are they managing?

Answer: There are 31 CORs across the House who manage 94 contracts. This includes House Officers.

Question 9: The Committee understands a new COR training program was implemented last year. Do you believe the training give CORs the education and tools necessary to execute their responsibilities?

Answer: Yes. The CAO's Chief Procurement Officer drafted new COR training curriculum to better assist CORs in performing their required duties. The improved training is designed around House operations and better equips CORs with the tools necessary to execute their responsibilities. The new curriculum is also taught by the Chief Procurement Officer (CPO) and now provides CORs with the opportunity to discuss issues with the CPO directly as well as with contracting staff during the training.

Question 10: Please give us a status update on the FY18 audit.

Answer: The FY18 financial statement audit is in process and the CAO anticipates results soon. The CAO is closely monitoring the progress of the financial statement audit and will provide an update on the audit results and any matters once they become available.

Question 11: Management of capital assets has been a consistent issue in previous audits and currently identified as a significant deficiency. Has any progress been made addressing this issue?

Answer: The House has long struggled with managing its assets. Even though auditors have identified significant deficiencies with the House program since FY13, it is more than likely the deficiencies existed well before then. To address the long-standing challenges associated with asset management, the CAO has recently taken the following actions:

- Established an Asset Management Compliance group to improve review of financial statement information and processes
- Implemented procedures that include a review of all capital asset purchases and disposals
- Implemented monitoring controls for all processes related to capital assets
- Performed annual inventories of all House capital assets in 2017 and 2018 with 99% accuracy
- Implemented two key technology modernization initiatives:
    - IT Asset Management – a perpetual inventory self-discovery tool for network-connected computer equipment and devices
    - Bar Code Scanners – a system that expedites and reduces human error in asset receiving, transfer, inventory, and disposal processes

Question 12: Has the west coast Point of Presence (POP) program cut response time?

Answer: Yes, the new West Coast POP program has reduced roundtrip times for internet traffic to, on average, 120 to 130 milliseconds. Offices are now experiencing response times in the 20 to 40 millisecond range.

Question 13: How many district offices are using VOIP connections?

Answer: 247

Question 14: Do all district offices now have a broadband connection?

Answer: Yes

Question 15: Since 2011, how much money as the CAO invested in retaining consultants to assess the voucher processing and payroll and benefits components of the Finance office?

Answer: In 2016, after operational irregularities and inconsistencies within the CAO's Office of Finance were identified, the Committee on House Administration encouraged the CAO to initiate an independent organizational assessment of the department. In September 2016, the Office of the Chief Administrative Officer awarded a contract to an independent firm to assess the capability and capacity of the Office of Finance to provide

customers and stakeholders with the support and information they require to fulfill their constitutional duties. The cost of the contract was $855,535.

Question 16: Since 2011, how much money has the CAO invested in retaining consultants to assess and make recommendations to our asset management program?

Answer: Since 2011, with the concurrence of the Committee on House Administration, the CAO has invested $1,246,220 in contractor support to assist the organization with its asset management program responsible for tracking the House's over 60,000 equipment items assigned to over 1,500 House inventories spread across seven buildings in Washington, D.C., and over 900 district office locations.

Question 17: Has the e-voucher program helped reduce the number of voucher errors?

Answer: 100 percent e-voucher processing was mandated in October 2018. Automation facilitated by e-voucher decreases the potential for manual data entry errors, drives greater efficiency in workflow, and improves continuity of operations as e-vouchers can be submitted and processed by staff remotely. While the CAO has not seen measurable improvements in voucher processing error rates as a direct result of the e-voucher mandate, it believes the transition was a necessary modernization initiative that has improved House operations. The CAO will continue to identify and implement improvements to its voucher processing procedures.

Question 18: Please update the Committee on the Smart Pay 3 roll out and improvements that have been made to payment processing.

Answer: At the beginning of the 116th Congress, the CAO completed a successful transition to a new House Finance Card Program, which impacted all existing and prospective House Travel Card and Purchase Card cardholders and their financial administrators. The transition required negotiating a new credit card contract and issuing more than 1,000 new cards and account numbers. It also presented an opportunity for the CAO to improve internal House Finance Card Program policies, including card issuance and payment processes and training and certification requirements. For example, under the new payment process, all card transactions now load directly into the House's financial system so offices can create vouchers with just a few clicks, eliminating both time intensive data entry and potential human error.

Question 19: According to HISPOL 8.1, the House Security Policy for Mobile Devices, Critical Operating System Updates must be installed within 72 hours and general OS updates must be done within 10 days. The consequence for non- compliance is: "[d]evices that do not comply ... will not be permitted to operate and could be disconnected from the House network."
    a. In practice, how does HIR enforce this consequence?

Answer: Noncompliance is enforced using mobile device management technology called AirWatch. The technology detects when a House network-connected device does not meet specific criteria deemed non-compliant. If/when non-compliant criteria are detected on a House-connected device, the device is quarantined within AirWatch and blocked from accessing the House network.

b. How are non-compliant users notified?

Answer: All House Systems Administrators are notified about device security policy requirements 20 days prior to enforcement. When non-compliant devices are identified, the users are notified directly via email a minimum of five separate times prior to the device quarantine.

c. How quickly is a non-compliant device disconnected from the House network?

Answer: This action can happen immediately. However, HIR usually provides multiple notifications to the user community prior to taking action.

d. How many times has a non-compliant mobile device had to be disconnected from the House network?

Answer: Since the deployment of AirWatch, there have been two separate compliance enforcement events to date.

e. Short of disconnecting a device from the network, what other ways does HIR enforce this policy?

Answer: Notification of non-compliance and disconnecting the non-compliant device are the only methods of enforcement.

f. The policy states that non-compliant devices are "[not] permitted to operate," what does it mean that a device is "[not] permitted to operate"?

Answer: It means the device is blocked from accessing the House network and its resources via the AirWatch software, including work email, contacts, calendar, and associated work mobile applications such as Office 365.

g. Does HIR currently have the capability to automatically force a mobile device to update its OS? Does such a capability exist for any of the mobile device OSs?

Answer: Once Android Enterprise is fully rolled out to all House Android devices, AirWatch will be able to require these Android Enterprise-managed

devices to be updated automatically. This rollout is planned to be completed in 2020. This capability is not currently possible for iOS (Apple) devices due to technical controls in place from Apple. To acquire this capability would require a major change to how the House procures and distributes iPhones and iPads. It would require the use of Apple DEP (Device Enrollment Program). The Apple DEP is a centrally managed program where HIR would purchase all the devices, configure them, and then issue them to authorized House users.

h. The HISPOL discusses responsibilities and consequences for not updating critical flaws in the OS, but does not mention what to do about critical flaws in non-OS applications. Do the same policies apply? Should this be clarified?

Answer: HIR does not currently enforce updates to individual applications unless made aware of a significant vulnerability to a specific application through the required mobile device security app (Lookout for Work) or through another cyber threat reporting mechanism. If HIR is notified of a specific vulnerability, the user(s) will be contacted to update or remove the application. HIR does recommend that applications are routinely updated to the most current version and users turn on the auto-update feature on their device. HIR uses Lookout for Work for security monitoring of device applications and to detect and notify users when vulnerabilities are detected.

This protocol will be clarified in future House Information Security publications.

Question 20: It is the Committee's understanding that Multifactor Authentication for mobile devices is currently undergoing a limited roll-out and should be rolled out to all House mobile devices by the middle of this year:
a. Can you please provide an update of this progress?

Answer: The CAO rolled out a Multifactor Authentication product for all House mobile devices this past November for the Microsoft Productivity applications (Word, Excel, PowerPoint, etc.) and Box. This product is currently available to the entire House, and HIR is in the process of migrating House mail to the cloud (Microsoft Exchange Online) with Multifactor Authentication applied to all House mobile devices. This migration is scheduled to be completed in 2019.

b. What factors are HIR currently using for mobile devices?

Answer: Factors currently in use include: (1) a certificate issued to only the person for each mobile device that must be managed by the House AirWatch/Workspace ONE environment; (2) mobile single sign-on that requires the person to use a biological factor, such as their thumb print, or the device PIN.

c. What factors are HIR considering for mobile device MFA?

Answer: Additional Multifactor Authentication capabilities that could be used in the future include Mobile Push Notification and/or texting of an additional PIN, as well as integration with a token, a one-time password application, and adding specific IP ranges as a factor.

d. How do you plan to evaluate the various MFA factor options?

Answer: HIR will continue to work with the Committee and leverage current working groups such as the Technology Task Force to gain input from the user community on what MFA options are most palatable for the House community.

Question 21: It is the Committee's understanding that Multifactor Authentication for desktop computers should be in place for all House computers by the end of this year:

a. Can you please provide an update of this progress?

Answer: HIR is currently conducting an MFA pilot using a module of an existing (in House) product and evaluating available Multifactor Authentication options. The House community is using a component of this product today for Multifactor Authentication access to the NetIQ solution. HIR installed the additional MFA components specific to Multifactor Authentication for desktop computers and is testing the available methods. The plan is to rollout Multifactor Authentication for desktop computers as a pilot to 50 users by June 2019 and then to the entire CAO by September 2019. The CAO plans to be prepared to support the House-wide rollout by the end of December 2019.

b. What factors are HIR considering for desktop MFA?

Answer: The Multifactor Authentication product to be piloted provides many authenticators including card authenticators, PKI, RADIUS Client, YubiKeys, email, voice call, SMS one-time passwords, facial recognition and fingerprint, passwords and security questions, Bluetooth devices, and smartphone applications. It is possible to combine more than one authentication method to form an authentication chain where multiple factors are required.

c. How do you plan to evaluate the various MFA factor options?

Answer: HIR is validating whether available options are viable for the House environment from a technical standpoint. It will then work closely with the Committee and stakeholders across the House to demonstrate the viable options and obtain feedback and guidance on the specific options to use. The goal is to determine the most secure methods viable and provide users a handful of different options to choose from that are secure, user friendly, and supportable.

Question 22: When HIR purchased NetIQ for user account management in 2017, the Committee understands that the application also included the ability to authenticate users using Multifactor Authentication:

    a. How does this impact the deployment of MFA for desktops?

        Answer: The authentication capabilities included in the existing product will help expedite the deployment of Multifactor Authentication for House desktops.

    b. Should we expect HIR to be able to deploy MFA more quickly, if not, why not?

        Answer: The current plan is to rollout desktop Multifactor Authentication by the end of 2019. This timeframe allows for a consultative approach with stakeholders across the House to provide feedback and guidance.

Question 23: Identity and Access Management (IAM) was a major initiative of the House Technology Task Force started in 2017:

    a. What are some of the practical benefits our offices will see from this system?

        Answer: The Identity Hub will streamline the processes for entering, updating, and accessing employee identity-related information and improve controls for managing access to various House resources such as the House network, financial systems, and privileged accounts. Once complete, the House will have one reliable system of record that will improve data security and the efficiency of House business processes. For example, when an individual is hired, the CAO's Office of Payroll and Benefits will enter the initial onboarding information into the Identity Hub, which will then trigger workflows to other CAO departments and House offices responsible for various aspects of the onboarding process such as network account creation.

    b. Can you please provide an update on the implementation of this system?

        Answer: In May 2018, the CAO rolled out the Identity Hub integrated with the House payroll system for use during the onboarding process. During the transition to the 116th Congress, the Identity Hub was used to generate data files for the Office of the Clerk more quickly and with increased frequency than prior transitions. Working closely with the House Sergeant at Arms, HIR is piloting an integrated, entirely online badge request process that will eliminate paper forms and automate workflow approvals. The pilot has started with HIR and will expand to other select offices in August 2019. Integration with Active Directory is planned to begin in 2020.

Question 24: Recently the startup ArticleOne, which provided AI based voicemail transcription services to member offices, featured a significant outage that prevented some of their member office customers from getting constituent voicemails. It is the Committee's understanding that the company is now going to be shutting down and the remaining member offices are being moved back to the House voicemail system:

    a. What important lessons, if any, were HIR able to learn through the process of originally assisting member offices in integrating ArticleOne and then ultimately having to unwind the integration?

        Answer: The primary lesson learned is that balancing innovation and office technology demands with thorough vetting beyond cybersecurity is difficult. Going forward, the CAO can more rigorously vet a company's operational and financial sustainability prior to approving its technology for use. However, that would certainly slow the House-wide rollout of new technologies. One way to improve the vetting of technologies will be the technology innovation lab being created by the CAO where Member offices will be able to test, evaluate, and share innovative tools and ideas. The lab will also help House offices, including the CAO, better understand the benefits, risks, and challenges associated with emerging technologies before House-wide deployment.

    b. Service like ArticleOne, is undeniably beneficial, but probably only necessary due to a lack of innovation in our own telephone and voicemail service offerings, is HIR looking at ways to be more innovative in this area?

        Answer: Yes, as mentioned, the CAO's innovation lab will improve the ability to identify, acquire, and implement innovative technical services for the House that improve operational efficiency and save money. In the case of ArticleOne's services, HIR already had some of the capabilities provided by ArticleOne, including unlimited voicemail and voicemail to email conversion. However, the CAO acknowledges that it needs to improve the marketing of these services, so more Member offices can take advantage of them.

Question 25: There are startups, and members, that are interested in offering new innovative services to member offices. As innovative as some of these startups are, there is also a risk of these companies going under or having a significant outage:

    a. What is HIR's role in helping member offices when the worst occurs with one of these services?

        Answer: HIR is always available to answer questions, provide guidance and assistance, and coordinate action/communications between the House and vendors. This coordination might include, but is not limited to, legal and contract assistance, billing issues, technical assistance, new vendor selection, vendor transition, and communications. For Correspondence Management Systems under the Technology Services Contract or web services under the Master Web Services Agreement, the contractual terms

are standardized to protect the House, so we are better positioned to assist in a resolution. However, for any products or services where no contract exists, options are more limited.

b. What contracts does HIR have in place with these vendors to deal with the worst-case scenario?

Answer: For vendor services that fall outside of the Technology Services Contract (Correspondence Management Systems, maintenance, systems administration) and the Master Web Services Agreement, HIR has no contractual protections with uniform contract and/or legal requirements. When HIR becomes aware of offices seeking technology products or services from a vendor outside of its standard technology and web contracts, HIR offers to advise them on formalizing the relationship contractually in a way that protects the office and allows the CAO to intervene when needed. However, HIR is not a party to those contracts and does not play a formal role in that relationship.

c. If need be, could HIR confiscate/repatriate member data from a failed company?

Answer: The CAO can only confiscate/repatriate data from a vendor with a contractual agreement with the CAO.

Question 26: HIR has recently started setting up regional Internet Points of Presence (POP), which will allow district offices to reach the internet without their traffic having to travel all the way to Washington D.C. and back, which should increase Internet speeds:
    a. Where else is HIR looking to put a regional POP?

Answer: HIR is currently looking to place POPs in regional hubs with a large concentration of district offices that experience slow internet speeds due to various factors, including their distance from the East Coast.

b. It seems to me that the greater benefit might be when HIR combines the use of a POP with cloud hosted House services, what will the benefits be to district offices if/when that occurs?

Answer: HIR has been in discussions with Microsoft and Equinix to discuss their network topologies and how the House can leverage their partnership to enhance access and speeds to Office 365 (Microsoft Cloud). HIR is currently testing the feasibility of the integration of this technology.

Question 27: Currently HIR Technology Partners only support a very small number of the House's total member offices (about 30):

a. Is HIR currently able to take on more member offices should they want to sign-up?

Answer: Is HIR currently able to take on more member offices should they want to sign-up?

Answer: Yes, given HIR's current staff augmentation support, it could take on additional Member offices. However, the CAO believes that the program must first improve and mature before it is expanded and heavily marketed to House offices. While the CAO is eager to expand the program, it understands that first impressions are vital and that the rollout needs to be done methodically as to prevent any false starts and negative experiences.

b. What is the level of satisfaction these offices have with their Technology Partners?

Answer: CAO customer satisfaction survey results collected since January 2019 for transactional services provided by Technology Partners indicate that the average satisfaction score is 4.83 out of 5. This level of satisfaction represents a 24 percent response rate for recipients of transactional services and does not reflect levels of customer satisfaction for consultative services, which the CAO believes requires improvement. In April 2019, the CAO started to deploy satisfaction surveys for some of its consultative services – including Technology Partner consultations. Once a statistically significant sample is collected, the CAO will analyze the quantitative and qualitative service satisfaction data for its transactional and consultative services and make needed improvements and/or adjustments to the program.

c. How aggressively is HIR marketing its free IT support services?

Answer: The best marketing is being recommended to a Member by a colleague. New Members were advised of the free service during the 116th Congressional Transition activities. The fact that more offices did not request to use the free service means work must be done to improve the service. When a CAO service is good, offices spread the word. If the service is subpar, no marketing campaign, no matter how aggressive, will overcome a bad reputation. That said, the CAO acknowledges the need for an effective marketing campaign and will have one ready to deploy when the Technology Partner program is ready for expansion.

d. Are there cybersecurity benefits to having more member offices supported exclusively by HIR Technology Partners?

Answer: Yes. Technology Partners ensure clear lines of responsibility for IT as well as consistent adherence to cyber policies and procedures.

Question 28: HIR offers free website development to member offices, what percentage of members use this service?

Answer: Approximately 60 percent of Members use this service.

a. What is the level of satisfaction these offices have with the Web Systems team and end result?

Answer: The feedback on the service has been positive, particularly since the CAO improved its approach to processing site development requests. Starting this Congress, House Web Services has implemented a new paradigm whereby a web site development team is immediately assigned to a requesting office versus being placed in a queue. The new assignment paradigm has eliminated the waitlist and increased production speeds. This has had a positive result and has increased the demand for HIR's Web Services website development services.

b. How aggressively is HIR marketing this service?

Answer: HIR Web Services aggressively marketed this service during New Member Orientation and will continue to work with CAO Communications and Marketing on ways to market this service in the future.

Question 29: While some member office issues are able to be handled entirely by vendor/contractor or shared-employee IT support personnel, in general, how many technology support issues would you say still require HIR personal to assist or support the vendors and shared employees in order to resolve the issue?

Answer: There are some actions that only HIR staff can execute. These include adding devices to the mobile device management system (AirWatch), issuing SecurIDs, and approving equipment requisitions. Since January 2019, HIR has added 1,200 devices to AirWatch, issued 1,500 SecurIDs, and approved 745 requisition forms. Additionally, there are several complex troubleshooting issues that routinely require HIR support, such as assisting with integration of third-party vendor products within the House environment (cloud products, telecom, etc.), and mobility applications, among other items.

Question 30: It is my understanding that HIR is currently reviewing its Security Policy for Protecting House Data in Cloud (HISPOL 17) to increase the transparency and efficiency of the reviewing process for authorizing the use House Data in cloud services. What kind of changes is HIR looking at?

Answer: HIR refined the scope of its cloud security policy review as defined in HISPOL 17 by focusing on systems that store House data versus systems that only

store publicly shared data (i.e., social media, email marketing tools, etc.). HIR has streamlined the review process and intends to leverage a cloud registry that includes cloud product risks.

Question 31: A number of member offices unofficially use cloud-based products in unauthorized ways for example using cloud word-processors to work on legislation or cloud based online forms to capture signatures for appropriations letters. Of course, the desire to use the products is understandable because they offer many benefits, but there is significant risk to offices that do this. Will upgrading to Office 365 be able to provide member offices the benefits of these cloud services without the same level of risk? What are some of the biggest benefits that member offices can expect to seem from upgrading to Microsoft Office 365? What are the benefits to the House as a whole?

Answer: From a risk perspective, using Microsoft Word instead of unauthorized cloud-based word processors provides these benefits without the same level of risk. The Office 365 suite is an approved House cloud service that incorporates the same collaborative benefits afforded by products like Google Docs with the following benefits. Benefits for the House as a whole:

- Ensures protection and integrity of House data and improved ability to support customers
- Improves the security of data through remote desktop software patches that prevent exploitation of known vulnerabilities
- Provides Speech and Debate protections incorporated into our contractual agreement with Microsoft to protect data in Office 365
- Available as an enterprise service from the CAO that any office can use readily rather than purchase other cloud services
- HIR Technology Partners provide full support to help customers with Office 365 free of charge

Benefits for individual offices:
- 5 Terabytes of secure cloud storage for each user with OneDrive
- Ability to edit files in real-time with multiple users
- Share files with users across the House via links rather than email attachments
- Ability to automatically save and access previous file versions without taking any extra storage space

Question 32: It is the Committee's understanding that House email services are on track be transferred to a Microsoft US government cloud data center by the end of this year. Could you please provide an update on this?

Answer: HIR is currently planning to migrate all users from on-premises Microsoft Exchange to Exchange Online before the end of the calendar year. HIR has prepared for this by successfully piloting this process and transferring email services for the entire CAO to Microsoft's U.S. government cloud data center(s) last year. HIR is planning to complete the House-wide migration during the August 2019 recess period to minimize the impact to customers.

Question 33: How will moving House email services to the cloud impact the cybersecurity of our email system?

Answer: Office 365's cloud email services are built to the highest compliance specifications, which is why a majority of the Executive Branch agencies are using Office 365, including the Department of Defense, as well as many Fortune 500 companies. Microsoft also obtained FedRAMP certification for Office 365 in the U.S. Government Community Cloud environment where House data is stored.

Question 34: What are some of the biggest benefits that member offices can expect to seem from moving email services to the cloud? What are the benefits to the House as a whole?

Answer: The greatest benefits of migrating email services to the cloud include:
- Increased inbox storage capacity: up to 100GB for a primary mailbox and unlimited archive storage

- New webmail access: Users will have a new option to access email from a web browser (portal.office.com) when connected to the House network and/or using the VPN client to access the House network from home or another location

- More stable email archive solution: To prepare for the large migration, all House user email data has been migrated out of Enterprise Vault to a larger, more stable archive solution – called the Online Archive

- Improved collaboration: Users can email file links versus files as attachments and have the ability to set file permissions after sending the link and can collaborate across mobile devices

Question 35: The Committee has long understood the House's investment at the Redstone Turner Data Center to be part of a strategy that allowed the House to minimize disruption to the users of the House network during disruptions, maintenance, etc. However, recent outages at the Alternate Computing Facility have impacted users experience for hours. Why is the House not using the Redstone Turner Data Center to provide uninterrupted access to the House network? What tangible benefits should ordinary users of the House network expect from our substantial investment at Redstone Turner? Was the Committee wrong in its expectation?

Answer: As the Committee is aware, the House has a business continuity and recovery posture that includes geographically dispersed data centers. This posture ensures House data is replicated to other locations to allow recovery from a disaster.   For many IT services, the backup location is Redstone Turner and all CAO data hosted on premises is migrated to the backup in real time.

Tier One services such as email, mobile support, and network and communications are active at both sites. While the network and associated communications paths require no

manual process to failover, some of the Tier One services such as email and mobile support do require a manual process. Their recovery can and has been executed quickly – usually in a matter of minutes. However, the Committee is correct that technical anomalies complicated failover during recent power outages at the Alternate Computing Facility. The CAO believes these anomalies have been resolved.

The CAO moved the primary location of many IT services to Redstone Turner. Redstone Turner is a highly reliable Tier 3 facility and has proven invaluable during the recent challenges at the Alternate Computing Facility.

Finally, it is worth noting that the CAO has adopted an aggressive cloud strategy and is actively moving email, storage, and public facing websites to the cloud, improving the resiliency of these services.

Question 36: HIR is about finished with its House Cloud Strategic Plan, could you please discuss some of the benefits of moving House services to cloud providers?

    a. What is the timeline for implementing the policy?

    Answer: HIR has developed a Cloud Roadmap that tracks critical path actions for implementing the Cloud Strategy. HIR has already begun executing on the Roadmap and will continue to do so over the next few years. Some short-term deliverables on the Roadmap include:
- Microsoft Office365 (end of 2019)
- A new learning and recruiting platform (mid 2019)
- House website migrations to the cloud (mid-late 2019)
- Cloud Access Security Broker (mid 2019)
- Cloud enablement of House institutional vendors (CY19-20)
- Continued workload migration and tenancy maturation (2020 and beyond)

    b. How does moving these services into the cloud impact House cybersecurity?

    Answer: Moving services to the cloud provides greater access to the latest hardware, timely security patching and updating of software, and around-the-clock monitoring of the sites and infrastructure allowing House cybersecurity staff to focus more on critical tasks and customer needs. Additionally, the cloud provides robust resiliency across multiple data centers ensuring the services are always available. HIR's cybersecurity program is evolving to account for the shift to the cloud by prioritizing FedRAMP authorized solutions, developing security and risk management policies and frameworks that work within a cloud environment, and implementing security tools that are purpose-built to maximize visibility and control of the cloud environments.

    c. Will there be some services that will continue to be hosted in House data centers?

Answer: Yes, House data centers will continue to be leveraged for certain workloads and capabilities.

d. What analysis is HIR doing to determine which services hare hosted in the cloud and which are hosted in House data centers?

Answer: HIR has developed an Application Rationalization Framework to assist leadership with making data driven decisions about where to host specific workloads. This is in addition to HIR's cloud-first approach for procuring new Enterprise services.

Questions for the Record from the House Administration Republican Office

Question 1: Given the requirement to maintain a public campus, unique and extended protections should be required to prevent inadvertent or nefarious access to House information systems. What are the plans and measures being considered/implemented to provide additional protections against inadvertent data loss in public settings from House information systems, including from direct introduction of non-House systems to the network, over-the-air data capture/passive data-sniffing, non-House staff accessing non-attended systems, non-authenticated access (shared or stolen passwords/identities), and malicious file introductions?

      a. What steps are being taking to remediate possible insider threat types of activities?

Answer: HIR has made extensive investments in cybersecurity and network management platforms and toolsets to strengthen the House's cybersecurity capabilities. However, opportunities exist to further leverage this investment through continued implementation and optimization activities. Based on the current business and technical operating realities of the House, the largest vulnerabilities are employees, contractors, or other trusted parties who may intentionally or unintentionally try to harm the House through their approved access to the networks, systems, services, and/or data.

To mitigate this risk, the Office of Cybersecurity will implement an insider threat program and port control program to identify, assess, and respond to risks and events related to insider access. To address this over the coming months, the Office of Cybersecurity, in conjunction with other HIR stakeholders, will review the current toolset configurations, status, and reporting capabilities and better integrate the toolsets and reporting to enhance their value. Additionally, HIR plans to implement the following initiatives to help to mitigate the insider threat:

Short-term Initiatives:
- Enhance port, protocol, and service limitation controls
  - The goal is to obtain complete visibility of all devices accessing network resources, including the ability to identify House-owned or approved devices. Additionally, the goal is to develop the capability to control the network access of any device, including the ability to block, quarantine, or isolate risky or unapproved computing devices accessing House systems or resources.

Long-term Initiatives:
- Enhance wireless controls
  - The goal is to develop effective controls to prevent and detect rogue/unauthorized wireless devices and access points as well as effective management and control policies for wireless capabilities.
- Implement advanced data protection capabilities
  - The goal is to develop required policies, mechanisms, and detections to control the review, transfer, disclosure, or loss of information to unauthorized individuals inside or outside the House.

- Develop insider threat program
  - The goal is to develop methodologies, practices, and tools to detect, limit, and prevent individuals with authorized access to House systems from intentionally exceeding or misusing access to negatively affect the confidentiality, integrity, or availability of House systems or resources.

Question 2: Phase 1 of the new child care center was opened this January. While you have physically expanded the facility have you had the opportunity to examine and evaluate the operations of the Center?

  a. What changes, if any, have been made to operations? Has the curriculum been reviewed?
  b. Have you experienced any major concerns from the parents who bring their children there?

Answer: The major operational changes are new positions created for the expansion that ensure continuity in child development and safety and provide improved services for enrolled children and their families. For example, Age-Group Coordinators have been added to the administrative team and are dedicated to each of the three age groups (infant, toddler, and preschool). They provide more oversight and support to the classrooms and spearhead curriculum decisions and enrichment opportunities for each of the age groups. The Nurse position has been added to provide more oversight to health and safety within the Center, and dedicated kitchen staff allow the classroom teachers and the administrators to focus on the children and families.

As the Center continues to adapt to its new space and prepare for its second expansion, it will continue to engage in an ongoing process of program improvement. That includes collecting data about practices and customer feedback and using that information to create plans for improved operations and enrichment opportunities.

The vast majority of parents have been very positive about the expansion. The bulk of parent concerns raised since the Center expanded to the O'Neill House Office Building have centered around parking and security. Some concerns that came up about the physical space have included the positioning of classroom telephones/telephone cords, the hardwood floors for newly mobile infants, and the weight of the doors into and between classrooms as well as the main entry door into the O'Neill Child Care Center space. The Center's administrators are working with the Architect of the Capitol, House Sergeant at Arms, and U.S. Capitol Police to address those concerns.

The Center also receives the occasional parent concern about typical child development/child care issues, including sleep and other routines, contagious illness, biting, and other challenging behaviors. For example, concerns have been expressed over infants acclimating to the new crib area that does not have floor to ceiling walls. The design ensures that caretakers can supervise infants by sight and sound at all times as required for the Center's continued accreditation by the National Association for the Education of Young Children. Working within the appropriate confines, the Center's faculty has and will continue to work with parents to address their concerns and help children

successfully and safely transition to their new environment.

Question 3: The House's Wounded Warrior Program is one of the most popular initiatives. Currently the program has a balance of nearly $7 million dollars and is requesting another $3 million dollars in FY2020. Why can't we spend the money? It is not because of a lack of disabled veterans seeking employment. Would you recommend any program changes to make this hiring process more efficient?

Answer: Since its inception, more than 250 disabled and/or wounded veterans have participated in the Program. Since 2017, the Program has continuously set records for the number of participating Fellows. In January of 2017, there were only 35 active Fellows in the Program. As of May 6, 2019, there were 61 active Fellows in the Program. Another 16 Fellows are scheduled to start on June 3rd, 2019 and as many as 10 more will start in July 2019. It is anticipated there will be close to 100 active Fellows by the end of December 2019.

With record levels of participation coupled with a rising average fellowship salary, which has now reached $47,000, the Program anticipates annual spending in calendar year 2020 will approach $5 million dollars. As such, assuming funding levels remain flat and fellowship participation continues to grow, the Program will not need to request a funding increase until FY 2022 or possibly FY 2023.

The Program's recent growth is due, in part, because of its improved recruitment efforts. The CAO is also exploring options to rebrand and better publicize the program. The CAO believes that there are other ways the program can improve, specifically in areas related to Fellow placement in district offices, the timing of applicant selections, and Fellow training opportunities.

The program's administrators generally find the veterans who would benefit the most from the Program's career transition assistance are in congressional districts around the country. Our fellowships provide a unique and often life-changing opportunity to veterans in cities like Cheyenne, Maryville, or Woodstock. Notwithstanding the importance of the legislative and oversight activities occurring on Capitol Hill in D.C. offices, the knowledge, skills, and abilities gained by Fellows in the district offices can also afford our veterans with valuable professional experiences.

Veterans in district offices forge partnerships with key stakeholders from local, state, and federal government agencies as well as non-profit organizations. The training and experiences gained by working in the district offices make the veterans from our Program a viable employee in their home area once they complete their fellowship. In fact, over the history of our program, most veterans from district offices have moved into a full-time role in their local community.

Currently there is no time limit as to how long offices have to make a hiring decision. There are offices that may take nine or ten months to make a hiring decision despite receiving a considerable volume of qualified applicants. Limiting the timing of applicant selections would benefit the applicants, the participating office that could use the

Fellow's support, and the other Member offices that have expressed interest in the program and are waiting for an opportunity to participate themselves.

Finally, the CAO believes that allowing Members to use their MRA on their office's desired training would help enhance the Fellows' contributions to their respective offices. Currently, Members are at liberty to utilize their MRA to enhance the professional development of their permanent staff. This may include staff attending conferences, forums, seminars, or other training not readily available to House staff. Training not only fosters good morale and job satisfaction but also increases the skill sets for all who participate.

Members recognize the inherent value of their Fellows and are often committed to hiring their Fellows following the completion of their two-year assignment. Accordingly, Members would like to invest in the professional development of their Fellows as if there were their own staff. This has elicited an increase in requests from Members to use their MRA to send their Fellows to seminars, conferences, etc.

As we move into 2019, the Program will continue placing a premium on professional development by expanding the orientation program to five days. Additionally, the Program is creating an advanced orientation program for seasoned Fellows to enhance their understanding of House operations.

Although the Program has an outstanding professional development program, it lacks the ability to target training for the specific needs and interest of a Member office. As such, Members should be authorized to utilize their MRA to send Fellows for training, conferences, or professional development as they deem appropriate.

Question 4: Last year the Legislative Branch bill provided $20,000 per Member office for the sole purpose of paid internships, effective April 1 regulations authorizing it were implemented. Currently, how many Members are taking advantage of this program?

Answer: As of the end of April 2019, 146 Member offices are employing House Program Interns.

Question 5: Last year the Office of Employee Advocacy was created to offer assistance to employees as they navigate the Congressional Accountability Act's dispute process. That office falls under your organization. How has the roll-out of this office gone? Are staff taking advantage of the office's services?

Answer: The rollout of the Office of Employee Advocacy (OOEA) has been successful. Since hiring the Director of the OOEA in September 2018, the CAO has retained experienced employment and litigation attorneys. As of May 2019, the OOEA composed of four attorneys (the Director, one Senior Associate Counsel, and two Associate Counsel) and a Paralegal, with a Legal Secretary to be added in late Spring 2019.

124

Working with the CAO's Communications and Marketing Team, the OOEA has engaged a targeted marketing strategy to inform the House community of OOEA's mission and its no-charge, complainant-side legal services. The marketing initiative has included various forms of communications media and outreach aimed at employees located in Washington, D.C., and in district offices across the country.

Since opening its doors, the OOEA has counseled and/or represented House employees on a wide range of matters. It has handled 97 legal issues and cases that House employees have presented to the OOEA for consultation, advice, or representation. Employees across the country and across the House's business units are taking advantage of the OOEA's services, including employees in Member offices, Committee offices, and the offices of the various Officers.

The OOEA workload continues to grow as awareness of the OOEA grows.

Question 6: It is our understanding that last year the CAO's finance office was reviewed by an outside consulting firm. What were the recommendations from that study; when will they be implemented and how will they help Member offices?

Answer: An independent, comprehensive assessment of the CAO's finance division was completed in September 2017 and provided the CAO with 30 actionable recommendations. The recommendations focused on codifying the CAO's financial management framework, improving customer service, and human capital improvements – all of which will improve accuracy, accountability, and customer engagement. Since the assessment, the CAO has worked to implement the recommendations. For instance, The CAO is working on the ongoing development of its internal policies and procedures to be completed and deployed in May 2019. In addition, a pilot project is currently underway using in-house knowledge management technology for CAO employees to establish and share precedents and resolution experiences. The knowledge management initiative will aid in standardizing activities using the appropriate process, procedure, and policy documents and preserve valuable organizational insight. Implementation of all the recommendations is on track to be completed by end of 2019. The goal of this effort is for Member offices to receive more efficient and seamless customer experiences through routine transactional services executed by employees with improved operational knowledge and resources.

Philip G. Kiko
Chief Administrative Officer

**Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515–6860**

HB–28, The Capitol

MEMORANDUM

TO: The Honorable Zoe Lofgren
          Chairperson, Committee on House Administration

FROM: Philip G. Kiko
          Chief Administrative Officer

SUBJECT: CAO Recruiting and Diversity Strategies

DATE: May 15, 2019

This memorandum is in response to your request for information at the April 9, 2019, Committee on House Administration hearing entitled "House Officer Priorities for 2019 and Beyond." The information outlined below provides insight into the Office of the Chief Administrative Officer's (CAO) recruiting and hiring activities to ensure diverse, qualified candidates to serve in our organization.

The CAO Human Resources (CAO-HR) team is responsible for designing and implementing the CAO's recruiting and hiring program. With over 700 employees who execute a broad spectrum of services for the House, the CAO organization is inherently diverse. It employs accountants, engineers, technology experts, childcare professionals, and skilled laborers of varying ethnicities, gender, and educational backgrounds.

To ensure we recruit diverse candidates to deliver the many services the organization provides, the CAO adheres to its strategic plan employee goal to recruit from a growing and diverse group of applicant pools. We are currently deploying a new cloud technology that will enhance and simplify the recruitment processes for both prospective hires and hiring managers. Once deployed, the new system will free up CAO-HR resources that can be dedicated to expanding CAO diversity and inclusion initiatives in the 116th Congress, such as forging relationships with diversity-related professional associations, local colleges, and attending job fairs to continuously attract diverse, qualified talent.

### Strategic Planning Framework and Technology Upgrade:

The CAO's recruitment activities are guided by the CAO and CAO-HR strategic plans. As illustrated in the graphic, the recruiting and hiring efforts are directly linked through

Objective 4.1 of the CAO's Employee goal, which requires the deployment of a talent framework for our organization.

The CAO-HR strategic goal to "Recruit Talent" ensures the CAO organization has a rigorous process to recruit and hire qualified staff. These activities are guided by an objective to "Enhance the CAO's recruiting program by improving collaboration between HR and hiring managers, increasing applicant pools, and strengthening candidate assessment strategies."

CAO Strategic Plan

Emloyee Goal: Develop and implement a system to foster a professional and engaged workforce

CAO Strategic Plan Objective 4.1

Deploy a CAO-wide framework by December 2017 to guide how we recruit, develop, secure, and retain talent

CAO HR Strategic Plan Goals

| Recruit Talent | Develop Employees | Secure the Workforce | Retain Capacity |

By including specific language in this objective to "increase applicant pools" our team is focused on expanding our outreach activities to attract diverse talent into our organization. In 2018 alone, the CAO posted over 70 job announcements and filled 115 positions through our recruiting and hiring process. During these efforts, the CAO-HR team received and manually reviewed approximately 100 resumes per job announcement. Based on the number of applications, we do not believe there is a shortage of interest from candidates wishing to serve the CAO organization.

However, the manual nature of our processes coupled with the associated workload demands that we improve our recruiting and hiring program has stretched our team thin. To this end, we are currently designing a cloud-based applicant tracking system for deployment this summer. This new automation will (1) create more efficient processes; (2) enhance the experience for applicants, hiring managers, and the HR team (3) provide access to data and metrics to improve the way we recruit and hire a diverse talent into the organization; and (4) free up CAO-HR resources that can be dedicated to organizational diversity and inclusion initiatives.
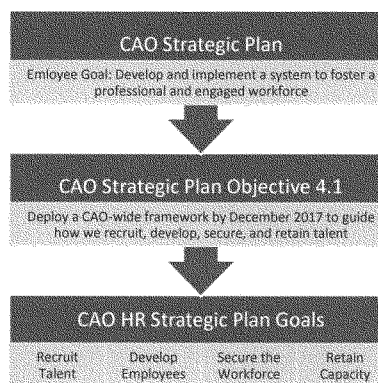
Accomplishments in the 115th Congress and planned activities for the 116th Congress:

115th Congress:

- Developed a comprehensive list of diversity related career sites and professional associations to expand where our jobs are posted.

- Increased the minimum days a vacancy announcement will remain posted from 5 days to 10 days to expand our applicant pool.

- Increased minimum number of interview panel members and required that one panel member be from outside the hiring department to ensure diverse opinions contribute to the hiring selection.

116th Congress:

- Deploying an applicant tracking system to automate our manual hiring process. The system will allow the CAO organization to:
  - Track key recruiting/hiring data (e.g., number of applicants received, number of qualified applicants, number of applicants interviewed, number of applicants hired)
  - Analyze how many applications we receive through each recruiting source (e.g. professional and trade associations, colleges/university, House.gov, USAJOBS, other)
  - Dedicate more CAO-HR resources to diversity and inclusion initiatives
- Building relationships with diversity related professional associations and career sites that align with the types of occupations within the CAO. For example, developing connections with the National Association of Black Accountants for finance-related jobs.
- Enhancing entry level recruitments by building relationships with local colleges, universities and trade schools.
- Attend targeted job fairs to increase diversity and outreach for mid-career and senior level positions. In March, CAO-HR and Finance attended a job fair for returning Peace Corp Volunteers.

###

116TH CONGRESSIONAL TRANSITION METRICS*

The 116th Transition marked the second largest freshman class in CAO history and a majority party change that increased typical transition activity workload to include transitioning House Committee and Leadership offices. Transition is one of the best examples of how the CAO puts its vision into practice.

*The claims, figures, and numbers in this document are current as of 2/28/19.

CAO VISION

To be an **ESSENTIAL RESOURCE** for every Member of the People's House through OUTSTANDING CUSTOMER EXPERIENCES delivered by **EXCEPTIONAL EMPLOYEES**.
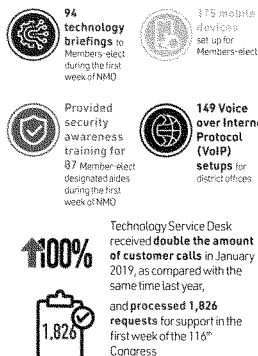

The 116th United States Congress began on January 3, 2019. There were 92 new representatives and 1 new delegate at the start of its first session.

54 CAO teams supported transition

CONSTITUENT ENGAGEMENT SERVICES
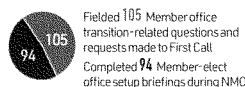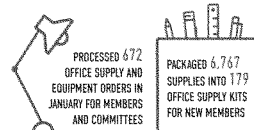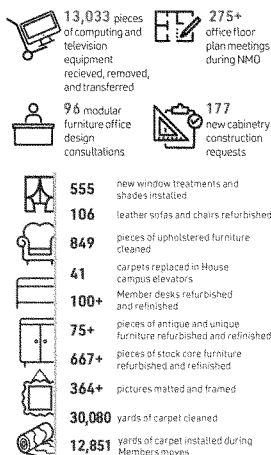
- 93 new Member websites
- 52 official Member portraits
- 29 departing Member photography archives created

TECHNOLOGY SUPPORT SERVICES

- **94 technology briefings** to Members-elect during the first week of NMO
- 175 mobile devices set up for Members-elect
- Provided **security awareness training** for 87 Member-elect designated aides during the first week of NMO
- **149 Voice over Internet Protocol (VoIP) setups** for district offices

100% Technology Service Desk received **double the amount of customer calls** in January 2019, as compared with the same time last year,

1,826 and **processed 1,826 requests** for support in the first week of the 116th Congress

---

OFFICE SUPPORT SERVICES

THREE DEPARTING MEMBER CENTERS SET UP TO TEMPORARILY PROVIDE OFFICE SPACE FOR 125 STAFF AND MEMBERS

- **13,033** pieces of computing and television equipment recieved, removed, and transferred
- **275+** office floor plan meetings during NMO
- **96** modular furniture office design consultations
- **177** new cabinetry construction requests

555	new window treatments and shades installed
106	leather sofas and chairs refurbished
849	pieces of upholstered furniture cleaned
41	carpets replaced in House campus elevators
100+	Member desks refurbished and refinished
75+	pieces of antique and unique furniture refurbished and refinished
667+	pieces of stock core furniture refurbished and refinished
364+	pictures matted and framed
30,080	yards of carpet cleaned
12,851	yards of carpet installed during Members moves

- **87** departing Member office move-outs — IN **13** DAYS
- **278** returning and new Member offices moves and 6 Leadership office moves — IN **26** DAYS
- **24** Committee office moves (48 consultations affecting over 1,000 staffers) — IN **19** DAYS
- **87** new Member office safety inspections — IN **6** DAYS

PROCESSED 672 OFFICE SUPPLY AND EQUIPMENT ORDERS IN JANUARY FOR MEMBERS AND COMMITTEES

PACKAGED 6,767 SUPPLIES INTO **179** OFFICE SUPPLY KITS FOR NEW MEMBERS

- **32** financial management office closeout consultations for departing Member offices
- **918** special events support requests completed
- **785+** district office leases and 20 vehicle leases reviewed and approved

Fielded **105** Member office transition-related questions and requests made to First Call

Completed **94** Member-elect office setup briefings during NMO

STAFF SUPPORT SERVICES

- **120** exit briefings conducted for departing Member, Committee, Leadership office staff
- **200** one-on-one Payroll & Benefits consultations conducted with new and departing Members of Congress
- **147** Member applications processed for official passports
- **201** resume and career planning consultations for individual Member Office and Committee staffers

CAO SERVICES ON THIS INFOGRAPHIC

Website Services	DC Office Furniture & Furnishings
Creative Services	Equipment and Inventory Management
Member and Staff Payroll and Benefits	
Passports	Special Events Logistics & Planning
Staff Training and Professional Development Services	Lease Administration
Financial Reporting	Customer Advocacy
Supply Purchasing	Technology Support
	Voice Services

Michael T. Ptasienski
Inspector General

386 Ford House Office Building
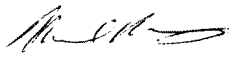Washington, DC 20515-9990

Joseph C. Picolla
Deputy Inspector General

Phone: 202-226-1250
Facsimile: 202-225-4240

Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990

MEMORANDUM

TO: The Honorable Zoe Lofgren, Chairperson
              Committee on House Administration

TO: The Honorable Rodney Davis, Ranking Minority Member
              Committee on House Administration

FROM: Michael Ptasienski
              Inspector General

DATE: May 14, 2019

SUBJECT: Response to Questions for the Record – "House Officer Priorities for 2019
              and Beyond" Hearing

Thank you for the opportunity to provide the Committee with an overview of the important activities of the Office of Inspector General (OIG) at the April 9, 2019 hearing titled "House Officer Priorities for 2019 and Beyond". I have included responses, below to the questions for the record, and would be happy to meet with you at your convenience, if you would like to discuss these or any other issues.

Questions for the Record from House Administration Majority:

Question 1: The Inspector General is responsible for overseeing the audit of the House's financial statements on an annual basis; what does that process entail?

    The OIG solicits and evaluates proposals before recommending the selection of the financial statement auditor. Once the contract is awarded, the OIG manages the contract with the external auditing firm. In addition to vetting all contractor staff, this responsibility includes ensuring the vendor performs in accordance with the contract terms, adheres to all House policies, and meets all contract deliverables. The OIG also serves as the liaison between the external auditor and all House stakeholders. This function includes coordinating meetings, assisting with document requests, and ensuring the follow-up on action items.

Question 2: You have testified before the House Subcommittee on Legislative Branch Appropriations that your funding request remains flat but are the needs of the House the same fc you to be able to operate without an increase in funding? If the needs of the House are greater how are you managing to provide adequate oversight necessary to fulfill your mission?

The operations of the House change over time and we have evolved our staff and expertise t meet those needs. For example, where significant time and effort had once been required to audit financial transactions, the automation of manual processes, increased analytics, and the use of electronic storage has made financial auditing more efficient and less resource intensive. The greater reliance on technology, across the House, has increased the need for our office to do much more auditing of the systems and networks that support House operations. We have also worked extremely hard to become more efficient internally by strengthening our back-office operations.

To date, we have been able to meet the changing needs of the House by utilizing existing resources. We continuously invest in and develop our staff to ensure we can meet current and future House needs while operating as effectively and efficiently as possible. Whenever possible, we utilize our internal staff for audit work. The OIG has contracting funds that ma be utilized to meet specific or urgent needs that cannot be fulfilled using our permanent staff

Question 3: One of the focuses of your office includes fraud prevention; have you seen any scams or frauds against the House for the 116th Congress? If so, what are they?

There has been one reported case where unsolicited boxes of toner were sent to a House office along with an invoice. The vendor then called the office demanding payment for the items. Working together with the Office of the Chief Administrative Officer (CAO) and Office of General Counsel (OGC), we have emphasized office education so Members and staff won't fall victim to these unscrupulous vendors. As recently as Monday, May 13, the CAO, OGC, and the OIG met with the House Professional Administrative Managers (PAM) group to provide an update and remind them of the resources they have available to protect themselves from these scams.

Question 4: What have you seen as the most popular scams against the House community in general? What steps has your office taken to address fraud or scams that are occurring in the House? Has law enforcement needed to be involved?

Since 2011, the House has received solicitations from toner, Yellow Pages listings, subscriptions, and domain name listing vendors. The toner vendors have been the most aggressive and prevalent. The OIG has taken the following steps to address these fraud scams:

- Educate and alert House offices through *Dear Colleagues Letters*.
- Provide information on fraud scams and prevention methods on the OIG website.

- Work with Office of General Counsel (OGC) and Office of Financial Counseling (OFC) to coordinate fraud prevention tactics.
- Provided names of vendors to OFC/ Accounting to prevent payment to these questionable vendors.
- Coordinated with the mailroom to stop delivery of toner from confirmed fraudulent vendors and return-to-sender.
- Refer offices that are being harassed by aggressive vendors to OGC.
- Monitor OIG hotline and respond accordingly.

In October 2011, there were discussions with the US Postal Inspection Service to determine what actions could be pursued against the toner vendors. It was revealed that gathering enough evidence against specific vendors would be very time consuming for House offices. In addition, these vendors change names and locations frequently, making criminal cases very difficult to prosecute. Given that information, we chose to instead focus on educating House offices. These efforts continue and I believe they have been very successful.

Question 5: With such rapid changes in technology cyber security remains a constant issue; what are some of the recommendations the House should adopt to better address cyber security?

Cyber Security is a major issue and one that requires constant vigilance due rapidly evolving threats and bad actors. The House needs to continue to invest in the people, processes, and technology that can help protect House networks, systems, and data.

The management of technology at the House is decentralized. Each office has a great deal of autonomy in the selection of what tools they use and provisioning access to systems. With this autonomy comes great responsibility. This presents unique challenges not found in other organizations. Typically, there is a central organization, staffed by experienced IT professionals, that have the overall authority and responsibilities when it comes to managing IT configurations and access. The mission and core competency of Member and Committee offices is not and should not be managing IT. I believe the House should provide and manage more IT services centrally.

In our technology environment, Members and staff are the most important defense against cyber security threats. Understanding the risks, being vigilant, adhering to House policies, exhibiting good cyber security practices, and reporting issues promptly is our best defense. Having strong, House-wide IT policies that are actively monitored for compliance and consistently enforced is an extremely critical facet of protecting the House.

Question 6: Do you know the last study that your office performed on strategic IT planning for the House? Is this an area that you think should be explored?

In 2016, our office looked at the overall structure of IT and how it is managed at the House. Succinctly, today, there is no central process to establish House-wide IT priorities, make strategic decisions, and prioritize IT investments.

Today, IT planning and direction is largely addressed independently within each House organization. As such, their IT decisions are primarily focused on their own mission and service priorities. The result is that IT planning across the House tends to be more tactical versus strategic in nature.

This is an area and a challenge that should be examined further.

Question 7: When is the last time that the IG has done a holistic review of the overall cybersecurity posture of the House and its Officers? Are there plans to undertake such a review?

In 2014 the OIG conducted a review of all House IT Policies (HISPOLs) and Publications (HISPUBs) against government and industry cybersecurity best practices to identify potential gaps or areas where policy could be enhanced.

Since that review, new computing capabilities and House-wide tools (such as Office 365) have been introduced. In addition, there have been numerous policy updates and several new IT policies. A review of these policies, by the OIG, is something that should be done periodically. I expect we will again be performing this type of review in the future.

Question 8: Are there better or more efficient ways to assess the cybersecurity posture of the whole House and its Officers than doing a single House-wide review?

Making sure the proper House-wide IT policies are in place, communicated, and enforced is critical to maintaining a strong cybersecurity posture at the House. These policies outline the roles and responsibilities each individual and organization has with respect to IT equipment, systems and networks. As these policies are universal and applicable House-wide, they need to be continuously evaluated to ensure they are comprehensive and clear.

Today, assessing cybersecurity practices is done by system, by process, or by organization. The OIG conducts numerous audits annually that look at various aspects of how cybersecurity program elements are implemented. Because each organization is responsible for implementing certain aspects of the program, the tools, people, and processes involved often differ from organization to organization. Assessing each organization and their respective processes is very time consuming and reflects the environment at a point-in-time.

Greater centralization of IT functions and responsibilities would streamline how IT is managed at the House. Processes would be much more universal in nature and managed in a consistent fashion. Operations and accountability would also be much less siloed and make assessing cybersecurity much easier.

Question 9: What is your plan to attract and retain a diverse workforce?

The OIG established a formal Diversity Plan in 2010 with the foundational philosophy of supporting workforce diversity. Our office embraces the philosophy that success requires a

culture that encourages understanding and utilization of the talents and capabilities of employees from all backgrounds and all organizational levels. Our plan is currently being updated as part of our regular review process for policy and procedures done for each new Congress. Updates to the policy incorporate recent changes in the House, to include aspects of CHA Res. 116-4.

Recruiting and retaining staff is challenging. My office employs both accounting and IT professionals. These skill sets are very much in demand across both the public and private sectors. We compete with federal, state, and local government entities as well as the many professional services organizations that operate in the DC area.

The employees of the Office of Inspector General come from a wide variety of backgrounds and organizations. We have staff that have joined us from the military, private sector, and other federal agencies. We only hire experienced professionals and identify candidates via public job announcements as well as targeted postings within the IG community and with professional associations.

When selecting staff, we look at the overall make-up of our organization and strive to have a workforce that looks like the world we live in. Having people with diverse backgrounds and experiences brings different perspectives to the work we do. It helps us look at problems from different angles and helps us appreciate different points-of-view. Succinctly, having a diverse workforce makes us better at our jobs.

Finding a diverse pool of candidates is a challenge that the accounting and IT professions face everywhere. Professional associations and other organizations are working hard to attract a broader section of the population into these professions. We all need to continue to find ways to attract and then retain these qualified professionals.

Questions for the Record from House Administration Minority:

Question 1: From your perspective as the House Inspector General what do you see as the biggest risks or challenges associated with House operations?

Cyber security is clearly the biggest risk at the House. The decentralized management of IT at the House makes protection of networks, computers, hand-held devices, and applications extremely challenging. Offices have a great deal of autonomy and responsibility when it comes to making IT decisions and managing their IT operations. More and more networked devices are added every day and each of these devices provides another potential avenue that can be exploited.

Making sure systems are patched and updated is just part of the challenge. The House cybersecurity professionals work hard to protect the institution, but they can't do it alone. User behavior and adherence to House IT policies and best practices is critical. Users need to understand how critical they are to the overall cyber security defense of the House.

Protecting user credentials, avoiding phishing attempts, using approved applications, protecting data, and not inadvertently downloading malware are extremely important.

Question 2: The inventory and more broadly asset management within the House has been a significant challenge for a number of years. This weakness has been noted numerous times on the House's annual financial audit. How can this be improved?

House asset management policies should be re-examined. The current policy has not been updated in many years, does not focus on risk, and is based upon the purchase price of the item. Items that meet a cost threshold (currently $500) are then tracked until they are disposed. In many cases, items have no monetary value, yet the House continues to track them.

The House should look at the risk associated with each asset type being purchased and determine if it should be continually tracked. A risk-based approach would likely focus on tracking those assets storing data or those easily sold and converted to cash. Accordingly, assets of little value or without House data would not be tracked. Processes can then be put in place to track the acquisition, transfer, and disposal of all items that have been deemed important versus trying to track a vast number of items that are not.

Question 3: The annual financial audit conducted by outside independent auditors is a function your office oversees. It is my understanding that you have changed auditing firms, why?

Every few years the OIG sends out a Request for Proposal (RFP) to public accounting firms to solicit bids on the House Financial Statement Audit. Historically the House has had difficulty in getting qualified firms to bid on the contract. There are several reasons for this.

Larger firms tend to view the job as too small when compared to other governmental audit opportunities. Many larger firms may also employ lobbyists and, for that reason, do not bid on the work. Smaller firms tend to lack the expertise and experience needed to conduct the audit. As such, the pool of potential firms that submit proposals and meet the qualifications necessary is very limited.

For the 2018 Financial Statement audit we selected a new firm that has the expertise to do the work and whose proposal was considered the best value for the government. The contract was issued for the FY2018 audit with four option years. At the end of that period (or if options are not exercised), the OIG will again send out an RFP for the next contract.

Question 4: How does your office reach its determination in selecting a financial auditor?

The OIG issues a Request for Proposal (RFP) that outlines the criteria for selecting the firm that will perform the Financial Statement Audit. The criteria consist of:

- The Independence of the Contractor

- Commitment to Meet Established Timeframes
- Qualifications and Experience of Contractor
- Technical Merits of Contractor's Approach
- Qualifications of Personnel
- Firm Policies and Procedures
- Price and Period of Performance

An Evaluation Committee is established to review all proposals. They also perform reference checks and select the most qualified firm which offers the best value to the House. This selection is then presented to the Committee on House Administration for approval.

Question 5: In your opinion, how often should we be recompeting the financial audit contract?

The latest contract for the Financial Statement audit was for one year with four option years. Base term contracts with option years are normal for these types of contracts. I think this is appropriate as it gives the House flexibility while also giving the vendor an incentive to perform and fully meet the terms of the contract.

If you have questions, please feel free to contact my office at (202) 226-1250.