EXAMINING THE ROLE OF SHARED EMPLOYEES IN THE HOUSE

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 12, 2018

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
32–657 WASHINGTON : 2018

COMMITTEE ON HOUSE ADMINISTRATION

GREGG HARPER, Mississippi, *Chairman*

RODNEY DAVIS, Illinois, *Vice Chairman*
BARBARA COMSTOCK, Virginia
MARK WALKER, North Carolina
ADRIAN SMITH, Nebraska
BARRY LOUDERMILK, Georgia

ROBERT A. BRADY, Pennsylvania,
Ranking Member
ZOE LOFGREN, California
JAMIE RASKIN, Maryland

EXAMINING THE ROLE OF SHARED EMPLOYEES IN THE HOUSE

THURSDAY, APRIL 12, 2018

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, D.C.

The Committee met, pursuant to call, at 11:16 a.m., in Room 1310, Longworth House Office Building, Hon. Gregg Harper [Chairman of the Committee] presiding.

Present: Representatives Harper, Davis, Comstock, Walker, Loudermilk, Brady, Lofgren, and Raskin.

Staff Present: Sean Moran, Staff Director; Kim Betz, Deputy Staff Director/General Counsel; Cole Felder, Deputy General Counsel; Dan Jarrell, Legislative Clerk; Erin McCracken, Communications Director; Jamie Fleet, Minority Staff Director; Khalil Abboud, Minority Deputy Staff Director; and Eddie Flaherty, Minority Chief Clerk.

The CHAIRMAN. I now call to order the Committee on House Administration for purposes of today's hearing on shared employees. A quorum is present, so we may proceed. The meeting record will remain open for 5 legislative days so that Members may submit any materials they wish to be included therein.

My opening remarks will be brief.

Today's hearing will focus on the practice by which multiple member offices share employees to perform administrative functions, such as finance or information technology services. The practice of sharing employees began in the mid to late 1990s and continues today. However, there had been concerns about the lack of oversight and supervision shared employees have in their duties. The Office of Inspector General audited the practice in 2008, and again, in 2012.

Today's hearing will provide this Committee with the opportunity to understand the history of the practice of sharing employees. Further, it will allow us the opportunity to review the current reporting and disclosure requirements imposed on shared employees and determine their effectiveness. Finally, the hearing will allow the Committee to understand the additional actions the House should take to ensure that all risks are addressed.

I yield to my colleague and the Ranking Member, Mr. Brady, for purposes of an opening statement.

Mr. Brady.

Mr. BRADY. Thank you, Mr. Chairman, for holding—and thank you for holding this hearing today.

Mr. Chairman, I have worked on the shared employees issue since I became Chairman in 2007. I had hearings on this topic, and we marked up new regulations to deal with this issue. I also supported the efforts of Chairman Lungren in 2012 to measure if what we were doing was working. We have more work to do.

I won't support an overall limit on the number of offices that share technology and finance staff that can support. We should discuss that limit. I also support a background check as a condition of access to the network. We need to explore what these background checks measure and what we do with the results.

I am very glad you have asked these witnesses here today. We have a fine group of House office in front of us. I consider Phil and Paul friends and look forward with our new inspector general once I learn how to pronounce your last name.

I look forward to the testimony, and I yield back the balance of my time.

The CHAIRMAN. The gentleman yields back.

Does any other Member wish to be recognized for the purposes of an opening statement?

Seeing none, we are honored to have yet another distinguished panel of witnesses before us, and I will now introduce those to the Committee.

Phil Kiko was sworn in as the Chief Administrative Officer of the House of Representatives on August the 1st of 2016. This is the second time Mr. Kiko is serving at the CAO. In the mid 1990s, Mr. Kiko joined the then-newly formed CAO, and his associate administrator for procurement and purchasing to help establish the procurement office. Mr. Kiko has a long record of dedicated service, both in the House and throughout the Federal Government.

Most recently, Mr. Kiko served as staff director and general counsel for two House committees, including serving on this Committee from 2011 to 2012. Mr. Kiko also has worked in two other House committees and served as chief of staff at a Member's congressional office.

I would also like to introduce Paul Irving, our Sergeant-at-Arms. Paul Irving was sworn in as the Sergeant-at-Arms at the U.S. House of Representatives on January the 17th of 2012 during the second session of the 112th Congress. He is the 36th person to hold this post since 1789. Mr. Irving previously served as an assistant director of the U.S. Secret Service from 2001 to 2008 and served as a special agent with the Secret Service for 25 years.

I would now like to introduce Michael Ptasienski, House Inspector General. Michael Ptasienski was appointed as the fifth inspector general of the United States House of Representatives on February the 15th of 2018. Mr. Ptasienski previously served in the Office of Inspector General of the House as the Deputy Inspector General, advisory and administrative services, and as the director, management advisory services.

He has been serving in the House since 2008. Prior to joining the House, Mr. Ptasienski spent more than 15 years working in consulting and management roles in the financial services industry, and has several professional certifications in accounting, auditing, risk management, and project management.

Again, I want to thank each of you for being here today with us. The Committee has received each of your written testimony. At the appropriate time, I will recognize you for 5 minutes to present a summary of that submission. You know how this drill works with the timer that is there.

We look forward to hearing from each of you. This is a very important hearing for us going forward. And the Chair now recognizes the Chief Administrative Officer, Phil Kiko, for 5 minutes.

STATEMENTS OF HON. PHILIP KIKO, HOUSE CHIEF ADMINISTRATIVE OFFICER, UNITED STATES HOUSE OF REPRESENTATIVES; HON. PAUL IRVING, HOUSE SERGEANT-AT-ARMS, UNITED STATES HOUSE OF REPRESENTATIVES; AND MICHAEL PTASIENSKI, INSPECTOR GENERAL, UNITED STATES HOUSE OF REPRESENTATIVES

STATEMENT OF HON. PHILIP KIKO

Mr. KIKO. Thank you for the opportunity to participate in today's hearing. The activity of certain shared employees and their technical service is one of the first issues that was brought to my attention when I became CAO. The House shared employees account for less than 1 percent of the estimated 10,000 House employees. Collectively, they work for roughly 75 percent of House offices.

Unlike the majority of House employees, the oversight structure of the technical services they provide is fractured and decentralized. Because they are not employees of any House officer, we are limited in our ability to take swift corrective action when non-compliance with House policies and technical standards are detected.

The problem is simple. Decentralized oversight leads to non-compliance and abuse of policies intended to protect the House. The solution is slightly more complicated, and one the House has been grappling with for the last decade. With that, at the direction of the Committee, in February 2017, the House officer working group convened, and in June of last year, issued a report identifying over 2,000 gaps in the management structure, the subsequent risk to the House, and reforms to mitigate those risks.

These gaps, in a broad perspective, relate to supervision and oversight of shared employees, or lack thereof, the delegation of tasks between shared employees, and the fact that they are sharing workloads and have informal supervisory agreements regardless of the employing authority. Improper vetting of the employees, and perhaps most problematic, the inability to enforce compliance with House information security policies. For example, the unauthorized assets to office data or commingling of data, the use of unsecured software, cloud service, email accounts, and equipment.

Many of these gaps are not necessarily new, but the risks associated with the gaps have changed and need to be addressed, particularly the risk that impact the House cybersecurity efforts. Cyber attacks, as you know, against the House, average 300 to 500 million each month. And the bookend to the outside threat is the insider threat.

Tremendous efforts are dedicated to protecting the House against to these outside threats; however, these efforts are undermined when employees do not adhere to and thumb their nose at our in-

formation security policy. And that is a risk, in my opinion, we cannot afford.

The working group concluded the most effective way to mitigate the risk of shared employee was to change the employment structure itself. And after the working group presented its recommendations, a Committee task force led by Representative Davis was created. It hosted multiple bipartisan listening sessions with Members on this topic, and I attended every one of those meetings. Members expressed a strong desire to retain shared employees as some of their duties can involve information that is sensitive in nature. However, Members were under the impression that, due to the technical nature of the duties shared employees, whether IT or financial, underwent a more vigorous vetting process, and they were also open to the CAO having a more hands-on oversight on compliance with House standards.

With this valuable feedback, a strategy was developed with the committee to mitigate risk and significantly modify the employment structure. It included the development of strict administrative standards for IT and shared financial administrators that would standardize the adherence to House policies and add additional oversight and compliance measures.

The CAO would be the centralized oversight entity with enforcement capabilities while preserving Member choice in hiring. It mirrors the current contractor model in that it allows for vetting individuals who will have privileged access to the House network, and it creates the ability to immediately revoke access for those who comply with House IT and financial policies. It doesn't mean they are revoked forever. It is revoked until they comply. Critical oversight capabilities that Member offices I do not think have the bandwidth to deal with.

The CAO stands ready to roll up its sleeves with the Committee and to close the gaps and greatly use the risks that are inherent in the current model.

Thank you very much.

[The statement of Mr. Kiko follows:]

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

April 12, 2018

CAO Submitted Testimony
April 2018

Introductory Statement
Chairman Harper, Ranking Member Brady, and members of the Committee, I appreciate the opportunity to participate in the Committee's April 12, 2018, hearing regarding the use of shared employees[1] in the House – one of the first issues brought to my attention when I became Chief Administrative Officer (CAO). I also want to express gratitude to my fellow officer, House Sergeant at Arms Paul Irving, for his leadership in the House Officer Working Group on Shared Employee Effectiveness and Risk Management (hereinafter referred to as the "Working Group"). Paul's expert security analyses and insight, coupled with valuable feedback from the Clerk of the House and the House Inspector General (IG), greatly informed the Working Group's approach to its analysis and subsequent recommendations.

As directed by the Committee, the Working Group started its analysis after the CAO's Office of Acquisition Management detected and flagged unusual invoices originating from five shared employees who served more than 30 House offices. The invoices, as submitted, were structured in a way to avoid the House's $500 equipment accountability threshold. Upon further investigation into the five shared employees' activities, the House IG discovered evidence of procurement fraud and irregularities, numerous violations of House security policies, and violations of the Committee's *Shared Employee Manual,* etc.

Though egregious, this behavior is not representative of the majority of the shared employees currently serving House offices. Many of them, much like the thousands of other House employees who serve this great institution, do so diligently and with great integrity and pride.

However, these violations and practices do greatly underscore the need to reassess how the House does business, and in particular, how it fulfills the technical and financial needs of House offices – some of which are currently provided, in part, by shared employees.

Vulnerabilities and abuses related to shared employees have been identified in the past. They were the impetus of the creation and adoption of the *Shared Employee Manual* adopted by the Committee in 2008 and updated in 2012. Prior to the creation of the Manual and since its adoption, the Committee has worked to address these vulnerabilities while simultaneously preserving the flexibility offices desire to hire individuals of their choosing to execute office functions that can be sensitive in nature – mainly office support for information technology and finances. Over the past decade, the Committee has worked to improve the controls over shared-employee activities.

Maintaining an effective model of governance requires constant assessment and reassessment. The analysis conducted by the Working Group at the Committee's direction and the input gathered by a task force created by the Committee are major components of the reassessment

[1] A "shared employee" is defined by the Committee on House Administration as an individual employed by more than one employing authority of the House. The policies included in the Committee's *Shared Employee Manual* applies to individuals employed by three or more House offices. In this document, a shared employee is defined as an individual employed by three or more House offices.

process and will inform any decisions made regarding the current governance structure over shared employees.

The House Officer Working Group on Shared Employee Effectiveness and Risk Management
On February 16, 2017, the Committee directed the CAO and the House Sergeant at Arms to form a House Officer Working Group on Shared Employee Effectiveness and Risk Management. The Working Group was to identify and examine the current gaps in the management of House shared employees that present risks to the House and to propose additional regulations and/or reforms to address the gaps.

In its analysis presented to the Committee on June 30, 2017, the Working Group identified multiple gaps within the current shared employee governing structure[2], including over two dozen gaps specific to: supervision and oversight; office employment and delegation of tasks; adherence to cybersecurity policies and enforcement; and administrative gaps that increase operational overhead for the House.

The supervision and oversight gaps cited in the Working Group's analysis stem primarily from the decentralized oversight structure of the shared administrators and the technical nature of their duties. Shared employees receive little to no day-to-day supervision from their employing offices, operating more like contractors and vendors that sporadically report to multiple offices in person or virtually. Because they are not the employing authority, House officers are poorly positioned to help with oversight. For instance, House officers cannot compel background checks or compliance with applicable House policies. Furthermore, when risks and/or noncompliance with House policies are identified, corrective actions by House officers is greatly delayed by the required coordination with shared employees' multiple employing authorities.

The gaps related to employment and delegation of tasks include problematic arrangements between shared employees themselves and noncompliance to required work agreements. For instance, some shared employees have developed teaming arrangements to sublet work assignments from various offices, even when one is not employed by the office, nor are they authorized to perform work for the office. In other instances, shared employees have developed supervisory/employee relationships between one another, even when they do not work for the same office. Additionally, there are shared employees who do not submit the required shared employee acknowledgement form with no apparent ramification, and/or perform work offsite without approved telecommuting arrangements.

The identified cybersecurity policy and enforcement gaps range from improper vetting of the employees themselves, to unfettered access to House accounts and use of non-approved

[2] The current House-wide "governance structure" for House Shared Employees is established by the *Shared Employee Manual* adopted by the Committee on House Administration. Additional applicable House policies include the House Information Security Policies, established by the Chief Administrative Officer (CAO) and approved by the Committee on House Administration, and the *Members' Congressional Handbook* created by the Committee on House Administration. House Rules are also applicable in addition to any policies adopted and enforced by each respective employing office, such as an employee handbook or office policies.

software and/or cloud services, to the use of unauthorized equipment. For example, too many shared employees have not undergone the recommended background checks, and far too many have privileged access to the House network with little to no supervision. House enterprise system management is generally not notified of the software they install nor the cloud services they use prior to application. Also, shared employees regularly work remotely using equipment and/or workstations that were not furnished by the government and that may not comply with House security policies. Shared employees also have comingled data from multiple offices and have failed to properly secure IT systems – placing Member data and the entire House of Representatives' IT infrastructure at risk.

The administrative overhead gaps identified by the Working Group commonly require a high degree of administrative work by House officers. For example, as shared employees regularly move on and off the payroll of various offices, significant resources are spent processing payroll authorizations and managing and reconciling health benefit designations and retirement transcripts.

Once it identified and analyzed these gaps, the Working Group determined that it is impossible to eliminate the vulnerabilities posed by the use of shared employees without making significant changes to the employment structure itself. The very nature of the decentralized structure fosters oversight inconsistencies and severely hinders the institution's ability to enforce compliance to the shared employee policies and House regulations intended to protect the institution and Members and staff.

The Working Group further concluded that replacing the shared employee management structure with an independent contractor arrangement would provide the CAO with the required authority to enforce compliance to House policies.

Committee on House Administration Task Force on Shared Employees
After the Working Group concluded its preliminary analysis and reported its findings, the Committee formed a task force that conducted multiple Member listening sessions conducted by Representative Rodney Davis. During these sessions, Members expressed a strong desire to keep shared employees on as House employees instead of contract employees. They specifically cited concerns over having independent contractors fulfill similar duties instrumental to their office operations, particularly office finance and personnel payroll actions that can be confidential in nature. Members expressed that they would always need an employee, albeit part-time, to assist with office finances and budget management and that it would be inappropriate to have that work performed by contractors.

The feedback provided during the listening sessions also indicated that Members were under the false impression that shared IT employees undergo a more rigorous vetting process than other House employees because of the technical and part-time nature of their duties. They were also generally unaware of the vulnerabilities created by gaps in the current governance structure and the abuse that had occurred.

Establishing Technology and Financial Administration Standards
Based on the preliminary analysis conducted by the Working Group and the feedback collected by the Committee's task force, an emerging recommendation was discussed to reduce risk to Members and the House by improving controls over the use of shared employees and in turn, compliance to the respective House policies. The new proposal would establish House Technology Administration Standards and House Financial Administration Standards requiring compliance by shared employees.

The House Technology Administration Standards would include strict requirements pertaining to shared employees' privileged access to the House network, how they provision access to Member and office data, and how they patch IT systems. The proposed standards would standardize how shared employees comply with House Information Security Policies (HISPOLS) as well as add additional oversight measures.

For example, HISPOL 16[3] requires that, "House Offices shall assign all Privileged Accounts the least amount of privileges necessary to perform the functions for which the account exists." However, HISPOL 16 does not define "least amount," allowing each respective office to determine the appropriate level of network access for its office IT administrator(s). As a result, shared IT administrators often have unnecessary direct access to Member office data that may not be needed to perform basic administrative functions such as patching or upgrading software.

Establishing standards would provide the House with an opportunity to define and enforce an exact and consistent level of access for shared IT administrators, alleviating House offices of designation and enforcement responsibilities.

House Financial Administration Standards would also be established and include strict requirements pertaining to shared employees' financial duties. These standards would also cover shared employees' technical use of House financial systems, their compliance with the House voucher documentation standards, and the proper separation of their duties to ensure sound financial management.

Both sets of standards would require that all shared employees undergo background checks adjudicated by the CAO, participate in ongoing training on House procedures and best practices, adhere to strong controls and practices preventing co-mingling of Member data and equipment, and adhere to all equipment procurement policies.

Enforcing strict adherence to House equipment procurement policies is necessary to identify and stop attempts at gaming the system, such as the fraudulent practice of "splitting vouchers" to avoid the House's $500 equipment accountability threshold. It will require the continued,

[3] HISPOL 016.0 *The United States House of Representatives Information Security Policy for Privileged Account Management and Security*. Approved by the Committee on House Administration September 2015.

increased scrutiny of submitted vouchers as well as greater control over interactions with equipment vendors.

Establishing the proposed standards would improve oversight of shared employees and improve enforcement – something Member offices are not well positioned to do as rigorously as required. They would also reinforce existing House information technology and financial policy requirements for both the employees and employing authorities.

Additionally, the emerging recommendation is to grant the CAO with the authority to revoke a shared employee's access to the House network if/when he/she fails to comply with the established standards.

Finally, for the proposed standards to be effective, it would be imperative that House offices that employ or would like to employ a shared employee require adherence to the established standards as a strict condition of employment. Strict adherence to the standards needs to be included in the job description of every shared employee responsible for information technology and/or financial services as a condition of employment and being granted access to the House technology infrastructure and its underlying data.

This new approach will help reduce the identified vulnerabilities while preserving hiring choices for Members through the creation of a centralized oversight component with the authority to require compliance to House policies.

Future Augmentation with CAO-Provided Technology and Financial Services
While it is believed that the proposed administrative technical and financial standards would help address known vulnerabilities, the Working Group's analysis suggests that the long-term goal should be to fulfill all House office information technology and financial service needs through employees directly managed by the CAO. To that end, the CAO is working with House stakeholders to incrementally enhance and expand its services.

Conclusory Statement
As mentioned, good governance requires constant assessment and reassessment and the ability to regularly adjust policies and procedures accordingly to maintain their effectiveness. It is equally important to ensure that whatever changes are considered, the underlying services provided to House offices continue to meet and exceed the needs of the House, whether through shared employees or CAO-provided services.

Although the services provided by shared employees are critical to Member office operations, there are known gaps and vulnerabilities with the shared employee governance and oversight structure. In 2008 and 2012 the IG identified these gaps, which led to Committee actions aimed at improving controls over House shared employees.

However, over time, the risks associated with the use of shared employees has changed – most notably the risks associated with House cybersecurity efforts. As evidenced by the recent

incident with shared IT administrators, significant gaps still exist that must be addressed. What may have worked in 2008 clearly is no longer effective to counter individuals and bad actors looking to exploit the current vulnerabilities for whatever reason. As the IG – as well as the Working Group – concluded, greater, more centralized controls are needed over shared employees and their adherence to House policies.

Though the initial recommendation of the Working Group was to eliminate the use of shared employees, feedback gathered from the Committee's task force highlighted the adverse impact implementing such a recommendation would have on Members' ability to hire employees of their choosing. Thus emerged the new, equally effective, recommendation to create strict standards that establish more oversight and a central enforcement mechanism for the CAO while also preserving Members' choice. This emerging recommendation strikes an important balance between both objectives.

I appreciate the opportunity to participate in the Working Group and contribute to the Committee's deliberations over improving the governance structure of House shared employees. Should the Committee opt to move forward and establish new technology and financial standards for shared employees as proposed, or take an alternate approach to address the identified vulnerabilities, please know that I stand ready to assist.

The CHAIRMAN. Thank you, Mr. Kiko.

The Chair will now recognize Sergeant-at-Arms Paul Irving, for 5 minutes for the purposes of an opening statement.

STATEMENT OF HON. PAUL IRVING

Mr. IRVING. Chairman Harper, Ranking Member Brady, and distinguished Members of the Committee, I appreciate the opportunity to participate in the Committee's hearing today regarding the use of shared employees in the House.

As you know, the House Sergeant-at-Arms serves as the Chamber's principal law enforcement officer. And from this perspective, shared employees present unique challenges.

Shared employees have access to systems, offices, and personnel of multiple Members, and can potentially create a greater risk than an employee who has access to only one office's systems. Shared employees may also have access to sensitive information technology or financial records.

As the House of Representatives has moved towards greater automation and increased use of digital technology, the vulnerabilities and risks have likewise increased. The risks posed by shared employees can be minimized by requiring background checks as well as robust internal controls. I would also recommend that shared employees be issued different ID cards.

Because of the greater risk of shared employees, it is critical that a shared employee be thoroughly vetted by the offices. However, Members are generally free to set the terms and condition of employment in their office. When an employee works for a single Member office, the Member can monitor the individual's performance and determine the level of trust and responsibility that should be vested in that individual. In certain respects, the Member assumes the risks of hiring the individual.

When an employee is shared among many Member offices, each Member is not as closely situated to monitor the individual's performance. The relationship between the Member and staffer is more attenuated, and knowledge about the employee's background is minimal. Thus, each Member potentially faces greater risk from the individuals who have access to sensitive information, technology, or financial data, as the Member is not as well positioned to vet or closely monitor the activities of the employee.

Currently, the Capitol Police provides criminal background checks for Members' offices upon request. When developing a policy concerning background checks, the Committee may wish to adopt or consider the scope, frequency of the investigation, and the adjudication or background of the background check.

Background checks are not a panacea, but they can serve as indicators that an individual is trustworthy or, conversely, potentially susceptibility to influences that could have negative repercussions for the entire House.

In addition to developing a uniform standard for background checks, it is also essential that there be uniformity in oversight as well as the institution of internal controls to ensure that all shared employees strictly adhere to the policies and procedures related to this unique position.

The CAO has put together a strategy for developing internal controls and ensuring the maintenance and uniformity of standards of shared employee conduct. I would support these recommendations by the CAO regarding the continued development and enforcement of these procedures.

I would also encourage all House offices to require strict adherence to the established standards as a condition of employment. Should an employee fail to comply with these standards, I fully support the CAO being granted the authority to revoke a shared employee's access to the House network.

One final area that can be leveraged to tighten security of shared employees is to provide a slightly different ID card to shared employees. Currently, ID cards are issued under one office, while a shared employee may work for many offices. Capitol Police officers can have difficulty identifying appropriate access when an individual's ID differs from the office in which they are working. If an ID card clearly denotes the employee of the shared staff, the officer can easily recognize that the individual might require further follow-up.

In sum, I want to thank the Committee for giving me the opportunity to testify today, and I am ready to answer any questions you may have.

Thank you.

[The statement of Mr. Irving follows:]

Statement of the Honorable Paul D. Irving
Sergeant at Arms
U.S. House of Representatives
Before the
Committee on House Administration
~~March 21~~, 2018
April 12,

Chairman Harper, Ranking Member Brady, and distinguished Members of the Committee, I appreciate the opportunity to participate in the Committee's hearing regarding the use of shared employees in the House.

Before beginning, I would like to say that it is truly an honor to have the opportunity to serve this institution, and I look forward to continuing to work with the Committee. I also wish to express my appreciation for my fellow House Officer Phil Kiko, the Chief Administrative Officer (CAO). Phil and his team have conducted a thorough and thoughtful analysis of the complexities of shared employees, and I greatly appreciate the opportunity to work with him on this issue. I appreciate the work and the input of the Clerk of the House and the Inspector General as well. As you know, the House Sergeant at Arms serves as the chamber's principal law enforcement officer, and from this perspective, shared employees present unique challenges.

Shared employees have access to the systems, offices, and personnel of multiple Members and thereby can potentially create a much greater risk than an employee who has access to only one office's systems. Shared employees may also have access to sensitive information technology or financial records. As the House of Representatives has moved towards greater automation and increased use of digital technology, the vulnerabilities and risks have likewise increased. The risks posed by shared employees can be minimized by requiring background checks, as well as robust internal controls. I would also recommend that shared employees be issued different ID cards.

Because of the greater risks of a shared employee, it is critical that a shared employee be thoroughly vetted by the offices. However, Members are generally free to set the terms and conditions of employment in their office. When an employee works for a single Member office, the Member can monitor the individual's performance and determine the level of trust and responsibility that should be vested in that individual. In certain respects, the Member assumes the risks of hiring the individual. The individual serves as a sort of "trusted agent" for the Member.

When an employee is shared among many Member offices, each Member is not as closely situated to monitor the individual's performance. The relationship between the Member and

staffer is more attenuated, and knowledge about an employee's background is minimal. Thus, each Member potentially faces greater risks from these individuals who have access to sensitive information technology or financial data, as the Member is not as well positioned to vet or monitor the activities of the employee.

Currently, the United States Capitol Police (USCP) provides criminal background checks for Member offices upon request. When developing a policy concerning background checks, the Committee may wish to consider the scope, the frequency of reinvestigation, and the adjudication of the background check. Background checks are not a panacea, but they can serve as indicators that an individual is trustworthy or potentially susceptible to influences that could have negative repercussions for the entire House.

I strongly encourage the Committee to require a stringent background check process for individuals who are serving as a shared employee. For example, a background check could vet the financial records for employees who are involved in procurement or financial accounting roles. Since many shared employees serve as financial administrators for Member offices, personal financial issues could indicate greater susceptibility to temptations that would put an office at risk. Likewise, repeated violations of information technology policies at a previous employer could raise greater levels of concern for employees who provide information technology services.

Specific types of background checks can delve even deeper into an individual's past depending on how the Committee would calibrate the background check process. Member and Committee offices already make decisions on the types of background checks that individuals should undergo when they submit requests for certain types of security clearances. The Sergeant at Arms will work with the Committee to determine the appropriate level of background investigation for any employees of the House.

The adjudication of background checks is an important tool to reduce risk. Currently, Member offices who request a criminal background check on an employee receive an employee's criminal records but little context on how to interpret the findings or appraise the risks of specific charges. Different offices have different standards and there is little uniformity as to what types of risks are acceptable. One Member office could choose to permit an employee to have access to sensitive financial information while another could determine similar results in a background check are disqualifying for employment. Developing a uniform standard for the background for shared employees would significantly improve the House of Representatives risk assessment for shared employees.

In addition to developing a uniform standard for background checks, it is also essential that there be uniformity in oversight, as well as the institution of internal controls to ensure that all shared employees strictly adhere to the policies and procedures related to this unique position. The CAO has put together a strategy for developing internal controls and ensuring the maintenance

and uniformity of standards of shared employee conduct. I would support these recommendations by the CAO regarding the continued development and enforcement of these procedures. I would also encourage all House offices to require strict adherence to the established standards as a condition of employment. Should an employee fail to comply with these standards, I fully support the CAO being granted the authority to revoke a shared employee's access to the House network.

One final area that can be leveraged to tighten security of shared employees is to provide a slightly different ID to shared employees. Currently, ID cards are issued to Congressional and support agency personnel. The ID cards allow the USCP to determine at a glance whether an individual is appropriately within an area.

Currently, the ID cards are issued under one office, while a shared employee may work for many offices. USCP officers can have difficulty identifying appropriate access when an individual's ID differs from the office in which they are working. If an ID card clearly denotes the employee as Shared Staff, the USCP can easily recognize that the individual would need further investigation.

I want to thank the Committee for giving me the opportunity to testify on these important matters. I would like to assure the Committee that the Sergeant at Arms stands willing to assist and provide the Committee its expertise and support in any way we can.

The CHAIRMAN. Thank you, Mr. Irving.

The Chair will now recognize our House Inspector General, Michael Ptasienski, for 5 minutes.

STATEMENT OF MICHAEL PTASIENSKI

Mr. PTASIENSKI. Thank you Chairman Harper, Ranking Member Brady, and Members of the Committee. I am honored to be here today in my capacity as Inspector General of the House.

My testimony today concerns two areas of shared employees: financial administrators and shared IT support staff.

Shared employees fill administrative and technical support roles for both Member offices and Committees through part-time positions. This model allows congressional offices to get the back office help they need without having to hire full-time staff. It does, however, introduce some significant risks.

Since 2007, we have conducted a considerable amount of work that has highlighted risks associated with these types of shared employees. Specifically, we identified risks associated with inadequate management oversight of shared employee activities, a lack of segregation of duties within offices, and shared employee noncompliance with applicable laws and House rules.

A particular concern is the role of the IT administrator. By its very nature, this role is highly sensitive and carries with it a whole host of risks.

The Office of Inspector General first noted risks associated with the shared employees in 2007 after a financial shared employee was able to defraud three Member offices for over $169,000. In this case, an employee had the authority to make purchases and controlled where items were delivered. In addition, they completed, approved, submitted, and—submitted vouchers for reimbursement. The same staffer also reviewed the office monthly financials and maintained all the office records.

This highlights a lack of segregation of duties. One employee should never have the ability to order items, receive the items, pay invoices, submit their own reimbursements, and reconcile the books.

Some shared employees may be on the payroll for as many as 20 offices. In addition, there have been cases where shared employees worked together in teaming relationships. These teams collectively handled the work of multiple offices. As a result, individuals may be performing duties for an office while being neither a paid employee or contractor for that Member.

In 2008, the CHA adopted Resolution 110–7 and subsequently published the shared employee manual in 2009, which placed specific limitations on shared employees that were based upon employment laws, House rules, and CHA's policies. This manual outlined several new requirements, including having shared employees sign an acknowledgment that they understood and would comply with the applicable rules and guidelines.

Not all shared employees, however, have been complying with these requirements. During a follow-up audit in 2012, we found that 45 percent of shared employees had not signed the required acknowledgment for understanding and complying with the manual. In addition, some shared employees continued to work as both

an employee of the House, and as a contractor. And as recently as 2016, we found shared employee teaming relationships still exist.

In any office, the system administrator is someone you place a great deal of trust in. This role is inherently risky due to the level of system access they have. They essentially hold the keys to the kingdom, they can create accounts, grant access, view, download, update, and delete virtually any information within the office. Because of this high-level access, an incompetent or rogue system administrator could conflict considerable damage to an office and potentially disclose sensitive information, grant access to others, perform updates, or simply delete files.

In the case of shared employees, this high level access spans multiple offices. We have seen that shared employees typically have a great deal of autonomy in conducting their work. In the case of IT administrators, they are generally an office's sole IT subject matter expert, and others may not have complete insight into the actions that they perform.

The existence of shared employee teaming relationships further increases the risk of having individuals who are not officially employed by a Member having access to their systems and data without the Member's knowledge.

Mr. Chairman, I thank you, Ranking Member Brady, and the Members of the Committee for this opportunity to highlight some of the risk and control weaknesses we have noted in the current shared employee model.

We look forward to continuing to provide advice to this Committee on issues of importance to the House.

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

The CHAIRMAN. Thank you, Mr. Ptasienski.

[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 12, 2018

Chairman Harper, Ranking Member Brady 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.

My office plays an important role in helping to ensure the integrity of House financial and administrative processes and identifying opportunities to improve them. My testimony concerns two primary categories of Shared Employees[1]; financial administration and Information Technology (IT). These Shared Employees provide administrative and technical expertise to both Member Offices and Committees through part-time positions. Shared Employees function essentially as independent contractors, yet they receive federal employee benefits. They actively market their financial administration or technology support services to multiple offices and negotiate the salary they will be paid with each employing office. Although this employment model allows congressional offices to meet their support needs without having to hire full-time personnel with the requisite skills and experience, there are significant risks to this employment model.

Since 2007, we have conducted a considerable amount of work related to House Shared Employees. Specifically, we identified risks associated with:

1) Inadequate management oversight over shared employee activities;
2) Lack of controls to ensure shared employees comply with laws and House Rules;
3) Lack of segregation of duties;
4) IT administrators perform sensitive functions and pose a special risk as they could violate the confidentiality, availability, and integrity of House information.

Financial Administration

The Office of Inspector General (OIG) first noted the risks associated with Shared Employees after inadequate oversight and a lack of segregation of duties allowed a shared employee to defraud three Member Offices of over $169,000 in 2007. In this case, the shared financial administrator submitted reimbursement vouchers for products never ordered, submitted invoices to multiple Members for duplicate reimbursement, and submitted vouchers for returned items and cancelled orders. This shared employee had the authority to make purchases, controlled where the items were delivered, was responsible for completing, approving, and submitting the vouchers for payments, entered the reimbursements into the accounting system, reviewed the monthly summary report of MRA expenditures, and maintained the records for office financial

[1] Shared employee is defined as a House employee who is simultaneously employed by three or more House employing authorities for more than 60 days during a calendar year.

transactions. This case led to the Committee on House Administration (CHA) directing the Office of the Chief Administrative Officer (CAO) to revise the Voucher Documentation Standards and advise Members to utilize segregation of duty controls in their office's financial functions. Essentially, one individual should never have the ability to order items, receive the items, pay the invoices, as well as reconcile the books.

Records have shown that Shared Employees may be on the payroll for as many as 20 offices. We had previously identified a financial shared employee who formed a teaming relationship with two other shared employees. The team collectively and interchangeably covered the work of multiple Member Offices. This resulted in individuals performing financial duties for and receiving expense reimbursements from a Member while not being either a paid employee or contractor for that Member.

Another risk with the shared employee model is that shared employees are not properly vetted. A background check is a reliable way of verifying claims made by job seekers during the hiring process and can highlight potential risks. The Shared Employee Manual recommends that Member and Committee offices request a Capitol Police Criminal History Records Check for potential Shared Employees. As of September 2016, however, we were only able to identify one instance where a shared employee had a background check performed by the House.

In 2008, the CHA adopted Resolution 110-7 which led to the development of a Shared Employee Manual that addresses specific limitations and conditions based on employment laws, House Rules, and CHA guidance. These guidelines outlined several new requirements including having shared employees sign an acknowledgement that they had read and understood the official guidelines.

Shared Employees, however, have not been fully complying with the requirements outlined in Committee Resolution 110-7. In 2012, we performed a follow-up audit and determined that 45 percent of the shared employee files we reviewed did not contain the required signed Shared Employee acknowledgement for reading and complying with the Shared Employee Manual. During 2016, we determined that teaming relationships were still ongoing, resulting in some shared employees working for House offices even though they were not on that office's payroll. Subletting or passing work to another individual not employed by the Member office violates U.S. Code and House Rules.

Information Technology (IT)

The role of a System Administrator is one that requires a great degree of trust and is inherently risky due to the level of system access they have within an office. System Administrators hold the 'keys to the kingdom' meaning they can create accounts, grant access, view, download, update, or delete almost any electronic information within an office. Because of this high-level access, a rogue System Administrator could inflict considerable damage to an office and potentially disclose sensitive information, perform unauthorized updates, or simply export or delete files. Additionally, a rogue System Administrator could take steps to cover up his/her actions and limit the possibility that their behavior being detected or otherwise traced back to them.

IT shared employees have a great deal of autonomy in conducting their work. They are generally an office's sole IT subject matter expert and most offices have no insight into the actions a shared IT system administrator could take. The shared employee model further increases this risk because shared IT system administrators may also have teaming relationships with other shared employees, which can result in non-employees obtaining access to a Member's systems and data without the Member's knowledge. Over the years, we have identified numerous instances where this has occurred.

Administrative Challenges

Maintaining the Shared Employee model at the House is also administratively challenging. Past OIG work disclosed that having shared employees working for multiple offices (with different salaries and titles for each office) is difficult and costlier for the CAO's Office of Payroll and Benefits to administer. Processing the volume of paperwork is time consuming and hundreds of personnel action forms are submitted to account for all of the part-time employment changes required to ensure the Shared Employees are paid correctly and that their service calculations and retirement cards are accurate.

Mr. Chairman, I wish to thank you, Ranking Member Brady, and the Members of the Committee for this opportunity to address the risks and significant control weaknesses we have noted in the Shared Employee model. 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 CHAIRMAN. We now have time for Committee Members to ask questions of each of you. Each Member is allotted 5 minutes to question the witnesses.

I will begin by recognizing myself for 5 minutes.

Mr. Kiko, I have a couple questions I would like to direct to you.

The House officer working group identified and the listening sessions confirmed the importance of protecting Member choice as it relates to certain services needed by Member offices.

In your opinion, how do we effectively mitigate the risk to the House that were identified in your June 30 memo and addressed in the working group's recommendations, while at the same time, continuing to recognize Members' employing authority? And are those two goals mutually exclusive of each other?

Mr. KIKO. No, I don't think they are. And what really came out of the working sessions—or the Member sessions headed by Congressman Davis was the fact that Members were very interested in having some choice. I certainly understand that. So what we sort of are thinking about is that the Members can hire shared employees. But the shared employees have to—the other thing that came out of that was that there was some understanding that maybe some of the employees were technically adept. They were required to follow all the House procedures and standards. So what we sort of thought we could do as—the CAO could establish standards for IT and financial services that everybody would have to adhere to. Then we would—and it would be standard. It would be the same for everybody. We would have standard compliance with regards so we could check to make sure that everybody's complying with what these standards are.

And then on the other side of the ledger, the Members would be able to hire who they wanted. But as part of those employee's performance standards, maybe there could be something in there that say they have comply, you know, with House policies. And then if they wouldn't, we could deny access, or we could tell the Member about it or elevate it to the Committee. But I think that is the way you can have it both ways.

The CHAIRMAN. Okay. On January 19th of 2018, Ranking Member Mr. Brady wrote to me highlighting a number of steps he believes can be implemented immediately to mitigate some of the risk.

Have you discussed these suggestions with HIR? And how do these steps fit in with the recommendations identified in your June 30, 2017 memo?

Mr. KIKO. I think a lot of those—in Mr. Brady's letter, I think of lot of those can be. Almost every one of them—all of them can be implemented. The one issue that we would have to work on a little bit is, you know, having a separate email for—every shared employee has a separate email account, and how would they email that, where would it go to? Would it—how do you separate it? Would it go into one server, or could it be disaggregated? We don't know.

But all those are fine. We agree with all those, and we can implement all of them.

The CHAIRMAN. And I am sure other Members will ask about this as well. But for you, Mr. Kiko, and for you, Mr. Irving, how impor-

tant and how effective will the background checks be that you anticipate having?

Mr. Irving may be the one to answer that.

Mr. IRVING. The background check, as I testified, is not a panacea, but certainly important as a vetting process to determine, you know, who would be most suitable to work on our sensitive systems.

Background checks take on a number of forms. Capitol Police will start off with an NCIC check, criminal history check, a credit check.

I would recommend that we explore a little deeper level of check as well, to maybe former employers to see if there were any anomalies, especially if it was on the financial side or IT side.

Not only—I wouldn't just focus on the background—the background check, but the adjudication of the check is important. Who actually is going to determine whether the employee is suitable. And we need to, I think, put some objective measure into that.

And then last but not least, probably a check every 5 to 7 years or so just to make sure that we check to see if the employee has had any issues, you know, since employment.

The CHAIRMAN. Thank you, Mr. Irving.

The Chair will now recognize Ranking Member Mr. Brady for 5 minutes for purposes of questions.

Mr. BRADY. Thank you Mr. Chairman.

My question is for all or anyone who would like to answer.

One of the ideas that I won't support is limiting the number of offices that shared technology and finance staff support. However, if you impose this limit on the overall number, you are going to raise the cost of the services provided to each office. So my question for all of you is do you support limiting the overall number of offices shared technology and finance staff can work for? And do you think there is a way we can help those offices that would experience an increase in cost, absorb that cost as we transition to this model?

Anyone.

Mr. KIKO. I support limiting the number of offices shared employees can support. Limits reduce the risk and the problem of diffused supervision. Where you set the limit is the hard question. Is it 10? Is it 20? Is it 5?

I do think that that the CAO can maybe help with that transition in a couple of ways. One is on the financial side. There are two initiatives that we are going to do that may work, and maybe e-voucher or something that replaces the existing scan paper. And the other is maybe if we launch a new financial portal to get offices more information, you know, that they could—there wouldn't be the need right now. A lot of the financial processes are very paper-intensive. We are trying to eliminate that.

But the issue of limiting offices I think is the—is how do you do that, and where do you draw the line on limiting the number of offices for shared employees? I don't know where that is. There has been as many as 20, 30. So that is all I have.

On the IT side, I think that, you know, in the end, it would be great if the CAO would provide services, that you wouldn't need shared employees for IT services. We sort of hope that we would

be able to do that in the future. I am not sure we are there yet, but we are trying to head that way.

Mr. BRADY. Mr. Irving.

Mr. IRVING. Not to place more of a burden on my esteemed colleague, Mr. Kiko, but certainly, some of this can be centrally managed. When we look at IT systems, I think a lot of that—those are services that the House offers, and I think that some of those services can be centrally managed which would, in fact, cut down on the number of shared employees.

Mr. BRADY. Thank you.

Do we know how many—how many average—do shared employees—how many Congresspeople that they work for? I mean, is there an average that they work for 30? 20? 10? I mean, do they vary?

Mr. KIKO. I don't really know. I don't know that answer at this point. I think there are some that are more and there are some that are very few. But I don't have the exact answer right now. I should have, but——

Mr. BRADY. It is hard to imagine that they work for, like, 20 and 15 Congresspeople and do an effective job. I mean——

Mr. KIKO. Yeah. I think it sort of depends up each individual offices, what are they doing and how much is being required of each office. That is what I don't know.

Mr. BRADY. Well, again, Mr. Kiko, for you—this question is for you. I think that you are doing an excellent job as our CAO. And do you have an estimate of how much money it would cost for your office to support the technology functions that shared employees and vendors currently provide our office?

Mr. KIKO. Well, I sort of looked into that a little bit, and I sort of believe that—we estimate that it would cost about $125,000 for 10 offices. So that is about 12,000. If we would—we would have an employee in HIR, they would support 10 offices. And so that would be about 12,500 or 13,000, 14,000 annually. So that is what we would think it would be if we would support it ourselves.

Mr. BRADY. Thank you.

Thank you, Mr. Chairman. And thank all of you. And I am very happy and proud to work with all of you. You do an excellent job.

Thank you.

The CHAIRMAN. Thank you, Mr. Brady.

The Chair will now recognize the Vice Chairman of the Committee, the gentleman from Illinois, Mr. Davis, for 5 minutes.

Mr. DAVIS. Thank you, Mr. Chairman, and thank you to each of the witnesses. I appreciate, Mr. Chairman, you tasking us with running the listening sessions that were bipartisan listening sessions. We had Members come in, Members who had shared employees, Members who were just concerned about the process, to get to know a little better about what these processes were. And I think Mr. Kiko laid out very effectively in his opening statement some of the concerns that Members had, and also, some of the perceptions Members had of possible background checks and other details that they thought may have been run through your office, the CAO, but in reality, they weren't done. So that is what gets me to my first question.

Mr. Kiko, you mentioned a number of compliance mechanisms that were suggested during those Member listening sessions and afterwards to help mitigate the risk of shared employees. And these suggestions included a badging authority through the Sergeant-at-Arms. And thank you, Mr. Irving, for mentioning that in your opening statement too. CAO developed committee-approved technology administration standards and financial administration standards; CAO control access to all enterprise systems; enforcement of new standards through the CAO controlled access to enterprise systems; CAO authority to terminate access for any shared IT or finance employee who is non-compliant with standards that currently exist; background checks, although at differing levels, as mentioned by Mr. Irving, for all IT and finance shared employees.

Would you describe, Mr. Kiko, how these implement—how these mechanisms could be implemented and enforced?

Mr. KIKO. Well, I think that—I think the first thing we have to do is to standardize, you know, what are the requirements for shared employees, whether it is IT or financial. And those standards should be high. It should be, you know, what is the normal industry standard for this kind of a function. Obviously, you have to apply it to the House.

And with regards to—and then there has to be a monitoring mechanism that the CAO would have to do. They could do spot checks on compliance. We are not talking about spot checks on getting into Member emails and stuff. We are just trying to see are they complying—you know, maybe every month. Are they complying with whatever the standards that we set, and the expectations that we set? And then if people are not, then we either give them a warning that they need to—they need to come into compliance. If they don't, we deny access or we elevate it.

Some of that stuff could be worked out with the Committee on what you want. I would say that is how you would implement it. It would require—it may require, you know, one employee, or two in the CAO's office, to make sure, you know, that everything is being done correctly.

Mr. DAVIS. I see a few of your employees sitting behind you.

Do you feel that the CAO has the ability to implement these suggested changes?

Mr. KIKO. Yes, I do. Yeah.

And I tried to limit the number of people that came here.

Mr. DAVIS. Well, you brought—Clocker was one too many. But that is okay.

Mr. Irving, I am very glad you mentioned the single badging authority. Can you expand somewhat on how you think that might help address some of the IG considerations that have been brought up before?

Mr. IRVING. It would just be one facet. When individual Members hire, their badge indicates where they are assigned or what Member they are employed by. A shared employee that has access to many Member offices is in a different category. And if a Capitol Police officer sees them in one area versus another, if someone questions them, not knowing that they are a shared employee could cause them to not follow up when they probably should follow up.

So only one other area of—just another facet. Certainly not in and of itself, something that is going to satisfy everything.

Mr. DAVIS. Great. Thank you.

One last question, Mr. Kiko. When we had our Member listening sessions, we talked about the lack of a compliance, complete compliance for the background and financial disclosure information and compliance measures that shared employees—the compliance rate they were at before the listening sessions. After you sent out some correspondence to the existing shared employees, what is the compliance rate right now for the disclosures and other information that we are requiring of them already?

Mr. KIKO. You mean on the financial disclosure?

Mr. DAVIS. The financial disclosures.

Mr. KIKO. I am not exactly sure what that is, because we did follow up. But that is more of an Ethics Committee issue.

Mr. DAVIS. Well, what about the information that you had?

Mr. KIKO. The information that we had is that, you know, most people are now in compliance, if not all. And I have had to send some emails out to people. Either you are going to get in compliance or we are going to cut you off. I did have one of those.

Mr. DAVIS. And you saw a great response to that of those who may not have been compliant?

Mr. KIKO. We are okay on this now.

Mr. DAVIS. Thank you.

The CHAIRMAN. The gentleman yields back.

And I would like to give a thank you to Rodney Davis as our Vice Chairman who has done yeoman's work and countless hours of working with—I know with each of you and working on this issue. So, Mr. Davis, we thank you for that outstanding work that I know we will bring to a conclusion at some point. And you will probably be happy when that happens. But we couldn't be in this position for the good of the House without your effort, so we appreciate it.

The Chair will now recognize the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Well, thank you very much. And thanks to each of you for your important testimony. And to you, Mr. Chairman and Mr. Brady, for convening this important hearing.

I think it is important to make a distinction between the kinds of shared employees that we have. There are technical shared employees that go from office to office, and they are primarily doing financial accounting work and IT work. And then there are, like, policy shared employees where the shared employee is actually moved around the payroll, but it is really for a shared policy goal. For example, you know, the Progressive Caucus or the Freedom Caucus might share the expense of a salary. Or State delegations have—you know, share the expense of a salary.

In 1995, it used to be, prior to 1995, that you could just—each office could contribute and just hire the person rather than going through this roll-around. I am not sure that what we did made any sense, honestly. It just increased the paperwork when it comes to policy issues. And that might be something to look at, Mr. Chairman.

But when it comes to the shared employees who are doing IT work or financial services, that is where we have the problem. And

I think it is important to make that distinction. Other Members have raised important issues relative to financial services.

I wanted to focus on the IT function. You know, for years, on a bipartisan basis, we have worked, Mr. Kiko, with your office, centralized services, ranging from magazine subscriptions to cybersecurity. It really doesn't make sense to have individual offices go out and buy their own furniture. We centralized that function. And so one of the concerns and, frankly, one of the complaints I have heard, and I suspect it is a resource issue for you, is that the CAO can be slow to support products that our consumers have moved to. And when that happens, Members and staff start using these products anyway. And then they circumvent security rules and regulations, because that is the product that they find useful.

And so I am wondering what HIR is doing to keep current with the latest tools available in the market? How do you identify those tools? Assess their security vulnerabilities, train your support staff to help with them? What role does HIR currently play in minimizing the risks that the status quo poses to the House, understanding that Members are going to move to new technology, and is that a resource issue for you?

Mr. KIKO. Well, we are constantly—we try to be on the cutting edge of new technology that Members are using. Many times a Member office will ask us about a new technology, and then we try to vet it. We try to see where the security issues are, you know, whether there is any problems, whether problems have been identified, you know, in the private sector when they have used stuff.

I have not checked to see whether this is a resource issue. But I know it is a very big problem, because, you know, we have all these technologies that Members would like to use. And then we read in the paper or we hear, you know, from some of our, you know, investigations and research that we do that there is a problem, you know, and stuff that has to be patched and all that, so—but it is a constant issue of, as you say, Members want the—some Members want the best and the latest. And sometimes stuff is vetted. If we find out that stuff isn't vetted correctly, we try to hurry up and try to do it to make sure there is not a problem, you know, with a whole——

Ms. LOFGREN. Right.

Let me ask you this: When you hire HIR staff, I think you examine their professional credentials, their certifications, their training for the function you are hiring them to perform.

Mr. KIKO. Yeah. It is very rigorous.

Ms. LOFGREN. And by the way, I think the IT staff I have interfaced with are excellent. They do a good job.

Now, when Member offices hire shared IT staff, are they required to meet the same training and certification that your own staff is?

Mr. KIKO. There is not a requirement for Members' offices, because they are the employing authority.

Ms. LOFGREN. Right. Maybe we should look at making those certifications a requirement if you are going to access the system.

Mr. KIKO. I support that.

Ms. LOFGREN. I am also interested in terms of shared IT staff. There is a concern that they don't always implement necessary upgrades or modifications or software patches.

Does HIR staff ever perform those duties if a shared IT staff drops the ball to protect our system?

Mr. KIKO. Yeah, we do. And we are, for the most part, responsible for that. But if a shared IT employee calls us, we will do it. It happens frequently.

Ms. LOFGREN. I see my time has expired.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Ms. Lofgren.

The Chair will now recognize the gentlewoman from Virginia, Mrs. Comstock, for 5 minutes.

Mrs. COMSTOCK. Thank you. And I thank the Chairman and the Vice Chairman for the work they have done on your going through and finding out the holes in the policies and you all working with that. So I really appreciate that in going forward.

And I know, you know, the public is rightfully, you know, very upset about how this was handled in the past and that this egregious example that is now being criminally investigated was allowed to occur. And I know, because of the criminal investigation, you aren't allowed to talk about that. But could you just address, you know, for public purposes, that as that criminal case goes forward and as that is resolved, that any additional suggestions or changes that might be apparent through what we learn from now can be addressed and making sure that whatever holes they were allowed to get through, I think it seems like we have identified a lot of them from what we know, but given that is still going forward, and we don't know everything, could you just assure for the public that that will be sort of an ongoing review when that is wrapped up?

Mr. IRVING. Congresswoman, I think everything that we have discussed today and the purpose of this hearing certainly is to get us there. And I will tell you that I am very, very confident that the CAO is putting measures in place and doing everything he can to put measures in place with the support of this Committee to mitigate some of those issues that caused us to be where we are today.

So, no, I am confident that we are certainly making a lot of progress. Ultimately, as you know, it is the balance between the Member interest and the governmental interest, the House interest, in really trying to come to a good place.

So I think we have accomplished a lot, even in the time during which this investigation has been ongoing.

And with that, I will ask Mr. Kiko if he wants to follow up. But I hope that satisfies you.

Mr. KIKO. No. I will just say that the abuses by certain shared employees have provided the CAO, and I think the Committee, with a roadmap on what needs to be closed. And that is what I want to do is to close the gaps.

Mrs. COMSTOCK. All right. No, and I appreciate that—you know, to the extent that that roadmap is public now, that you have been able to address that and just wanted to make sure, as we get more information, you know, that may not apparent at this point, that we can follow up on that.

So I thank you for the work you are doing on that front.

And I yield back.

The CHAIRMAN. The gentlewoman yields back.

The Chair will now recognize Mr. Raskin for 5 minutes.

Mr. RASKIN. Mr. Chairman, thank you very much, and thanks to all of our distinguished witnesses today. All of you have discussed different risks that the current situation presents to the House, including risks involving oversight, cybersecurity, physical security, money, and so on.

Do you believe that your offices have sufficient authority now under existing House rules to address those risks, or does the Committee need to consider providing additional authority to you in order to deal with it?

And maybe we just go right down the line.

Mr. KIKO. I would just say that, you know, we are in the process of working with the Committee to reduce the risk by giving the CAO a little more oversight authority over abuses. Now, this is just for the CAO purposes. And I think that if we have more authority and we can, you know, set standards, do compliance, I think that will greatly reduce the risk in cooperation with the Member and working with the Committee. Because right now, we don't really—because these are Member employees and we don't have a lot of authority to deal with that, and it just hasn't happened, even though we found about how the abuses can be—how the weak spots can be exploited, we think that will go a long ways.

Mr. RASKIN. Let me just follow up quickly with you, then.

Would it make sense—obviously, what we have got, you know, cherished traditions of Member autonomy and some constitutional background to that with the speech and debate clause, but would it make sense for us to generate more authority in your office or in some constellation of these offices, to deal with shared employees on the theory that if a Member wants to go outside of the usual situation of having an employee reporting directly to her?

Mr. KIKO. I mean, I wouldn't be opposed to that. That is sort of a fine line, you know, between CAO and Member autonomy. But I am in favor of exploring that. I think it would help.

Mr. RASKIN. Mr. Irving.

Mr. IRVING. I am certainly in agreement with the CAO. I think that, as I alluded to earlier, when the governmental interest is so heavy and when we get to cybersecurity, we really have a governmental interest. We certainly have to recognize the Member interest as well. But I am in favor of giving the CAO those—the authority so that, for example, to Congresswoman Lofgren's point earlier on standards, maybe we need to make sure that even though the Member is the employing authority, if they want to bring someone on to do IT, for example, they should comply with certain standards, have certain background. And the same with the internal controls. I think the CAO needs every internal control available to him or her to ensure that these employees are, in fact, complying with rules and regulations, and then have the authority, certainly, to take certain action even though they are employed by a Member. And I know it is a very, very careful balance.

Mr. KIKO. I don't want anybody to get the impression I am trying to grab more authority. I am trying to grab more power. That is

not the case here. I am just trying to walk a very fine line in conjunction with the Committee to see, you know, where that sweet spot is. That is what I am trying to do.

Mr. RASKIN. Great. Thank you.

Mr. PTASIENSKI. I think the—as the Chief Administrative Officer said, I think they are the primary organization looking at—or monitoring compliance with a lot of these finance and technology policies. And as such, they have got a tough job in trying to enforce those. And I think if there is—if he can't, and his folks, as they interact with offices, get people to comply with those policies, if he needs a stick, he may need a stick in some areas, and we would support that.

We put a lot of pressure as we make recommendations to the CAO to fix the various issues and so forth. And I have full appreciation for the tough job that they have in balancing some of the particularities of here working in the House.

Mr. RASKIN. Thank you very much.

I yield back, Mr. Chairman.

The CHAIRMAN. The gentleman yields back.

The Chair will now recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you Mr. Chairman.

My time is centered basically around one area regarding the working group. And I wanted to get your thoughts on that, both to Mr. Kiko and Mr. Irving, on the—briefly, you have described the objectives of the working group, how it conducted its work. And I know it has reached, I believe, six conclusions.

Could you talk about how that factors into your recommendations?

Mr. Kiko, let's start with you.

Mr. KIKO. Yeah. I think that on our recommendations we initially had said that we—you know, we went through all the abuses. We went through previous IG reports. The IG was part of the working group, and we initially had recommended an independent contractor model rather than—you know, as a way to preserve—as a way that we could better—feel better served, close the gaps with regards to risks.

You know, we have CMS services in the House. Some of them are employees that work for them, and they also provide IT services. We use that model because we have a direct relationship with the contractor, and if somebody's not working out, then we call the contractor and we cut it off.

But when we started the—you know, we met with Mr. Davis' group, there was concerns about that model. And so we decided to do the model that I just described where we would work in conjunction with Members' offices.

Does that make sense?

Mr. WALKER. Yes.

Mr. IRVING. And I will certainly agree with Mr. Kiko. Initially, our view was how do you put as much control, internal control and control over access to sensitive networks. So, you know, myopically we can say, well, we should just control the employee, but knowing that Members do want to hire some of their own people, we had to work with that and recognize that and appreciate that.

And I think we are in a good spot where we have—we are able to satisfy both concerns, which is ensure that our internal controls are safe, internal mechanisms for cybersecurity, but also allow Members the ability to continue to let Members, you know, hire people that they feel comfortable with.

The key is just ensuring that we have those internal controls, and sticking to them and that Members respect the CAO's authority to, you know, to—in a sense, discipline employees that may not be abiding by the rules.

Mr. WALKER. So, Mr. Irving, do you put more emphasis on the discipline in the internal controls, or do you place more emphasis—and Mr. Kiko can respond to this as well—on reducing the overall amount of privileged or shared employees? What is your ultimate recommendation?

Mr. IRVING. I would turn this over to Mr. Kiko, but my comment is, I would have as few people have access to those sensitive networks as possible. That is first and foremost. But some will need to, certainly depending on the Member and the committee they are on, et cetera. So those I would make sure that Mr. Kiko has the authority to ensure that those internal controls are met.

But I don't know, Phil, if you wanted to elaborate on that.

Mr. KIKO. I mean, I would just like there—from my perspective, there be a justification for the access that we are supposed to have. I am not necessarily trying to have limits, you know, at least on privileged access.

You know, people, other than shared employees have access. I just think there needs to be a good justification for what access there is, and also that they comply with whatever standards that we have. I am not really trying to grind them down into not—you know, into a number.

Mr. WALKER. That is fair. Fair argument.

Mr. Chairman, I yield back.

The CHAIRMAN. The gentleman yields back.

The Chair will now recognize the gentleman from Georgia, Mr. Loudermilk, for 5 minutes.

Mr. LOUDERMILK. I thank you, Mr. Chairman.

I appreciate the panel being here. I am a little confused though. Again, a guy with a military background, I am sitting here looking, Mr. Kiko is a chief, Paul is a sergeant, and you are a general. So I am not sure which one outranks who here.

But, hey, I appreciate the work that has been done here because this is an issue of grave concern, but also it is a balancing act. Because I think, as several Members have expressed, one of the strengths of our—this legislative body is the autonomy of each individual office, as compared to when I was in the State legislature.

Our staff was appointed to us, the limited staff we had. The Speaker of the House actually controlled who our employees were, and it really limited the autonomy you have. And I think that is one of the strengths that we have here is we are able to actually operate as our own entity without due influence—undue influence from the outside entities or leadership.

However, that strength also becomes a weakness when it comes to the finances, and particularly IT. And as the gentlelady from California spoke about, you know, policy not so much a concern

other than the access to the IT resources. So I have, in the last few days, tried to strike where is that balance?

On the IT side specifically, I had a couple questions, and I kind of like the direction that we are going. I spoke to Mr. Davis yesterday about what Mr. Kiko had defined earlier as a direction we may be going.

One of the—we brought up certification. You know, from an IT perspective, I can appreciate that. I think it is important that, you know, who you hire does know what they are doing, or maybe from the accounting and the finance side requiring a licensing or a certification, you know.

But still, that is more of a job performance aspect to me is that you—and being in the IT field, I am going to be able to decipher whether you really know what you are doing or not. My concern comes to the cybersecurity side and nondisclosure.

When we share employees, there is also an aspect to the autonomy is, I don't want that shared employee sharing with other offices what is going on with my office as well as disclosing to some entity privacy information.

Do we have or have we considered a confidentiality nondisclosure agreement that each of these shared employees have to sign, or some training to go through that spells out the penalties that—especially if they disclose, you know, information that we have on constituents or information we are working on.

And I will open that up to anyone. Is that something we have, or is that something that has been discussed?

Mr. KIKO. Well, I know we have a shared employee manual, and it requires nondisclosure. And so when the—you know, that is a requirement to be a shared employee that you are not supposed to disclose other Members' information. That is already a requirement that the Committee, at the request of the IG, had done and it is already in.

I don't know if there is a—they have to sign off that they received and they are going to comply with everything that is in the shared employee manual, but that is in that manual now. It is not a specific letter, but that is part of the manual as we——

Mr. LOUDERMILK. Does that spell out what penalties are, i.e., you can go to jail?

Mr. KIKO. There aren't any penalties.

Mr. LOUDERMILK. Is that something that maybe we should look at?

Mr. KIKO. Well, the only penalty would be termination, but perhaps. I am willing to pursue that, whatever the Committee would want to do.

Mr. LOUDERMILK. Mr. Irving.

Mr. IRVING. I think that goes along—Congressman, it is an excellent theme for some of the prior questions in terms of what can we do to enhance our internal controls and our policy. I think that is certainly one that I would endorse that we need to strengthen.

Mr. LOUDERMILK. Okay. I appreciate that.

One other question, wherever we get to with this, is this something that we would look at doing a new Member orientation to make sure that every new Member that is coming in is fully aware of the rules and responsibilities not only of the shared employee,

but their requirements as well? That may be something for a staffer.

Mr. KIKO. We would be willing to have that as part—and participate if that is what the committee wanted to do.

Mr. LOUDERMILK. Okay. I yield back.

The CHAIRMAN. The gentleman yields back.

I will recognize Mr. Davis for a follow-up remark.

Mr. DAVIS. Mr. Kiko, once again—actually, I am glad my colleague Mr. Loudermilk brought up compliance and nondisclosure.

Now, when we had our Member listening sessions, we did discuss—and hopefully, as a plan of action moving forward, we might be able to implement some penalties for noncompliance up to termination for noncompliance.

Do you think that would be easier to administer under the current shared employee rules and regulations, or under maybe some of the proposed changes we talked about today, running those compliance measures through the CAO, Sergeant-at-Arms, and House Administration?

Mr. KIKO. I mean, I think we should take a look at that. I think that however we can make compliance easier we should do. I don't—I think termination now, it is the shared employee, it is the Member's responsibility to terminate. And it still will be, but——

Mr. DAVIS. It will still be the Member's responsibility to terminate, but you would be able to, hypothetically, under the possible proposed guidelines, be able to revoke ID badges?

Mr. KIKO. Yes, we can revoke everything and then they can still be employed, but it would be a much different role.

Mr. DAVIS. Yeah.

Mr. KIKO. And you could give the Committee some more authority, too, on those kind of things when they see that.

Mr. DAVIS. Well, thank you for that suggestion.

And I just, again, want to say thank you. I know each of you have worked hard on this issue.

Phil, you have been in the room with us listening to Members. I truly appreciate the fact that through your testimony today, based upon previous suggestions and previous memos that have come out, that you listen to the Members.

And that is something that I just cannot say thank you enough for, because our job is to address the Members' concerns and do it in a way that is also going to address their employees' concerns.

I look out in the audience, and raise your hand if you are a shared employee. I hope each and every one of you understand that your Member's concerns were heard.

And I look out and I see one of my shared employees sitting here watching this, this hearing. Obviously, this is of concern to those who were already at that status.

But please understand, we have to do a better job of ensuring that we have better compliance, we have better standards, and so those of you who are working very hard as a shared employee right now can continue to do that job in the future, and not let those who aren't determine your fate, too.

So thank you again, everyone.

And thank you, Mr. Chairman, for the opportunity.

The CHAIRMAN. The gentleman yields back.

The Chair will now recognize the gentlewoman from California, Ms. Lofgren, for a closing remark.

Ms. LOFGREN. Yes. Just a quick question, but before I do, you know, we have examined ways to improve the shared employee situation, but we really, really said there is some value to it as well, because if you have to hire in each office a specialist on IT, that doesn't make a lot of sense.

So having some shared expertise, whether it is located in the CAO's office, or whether it is shared employees, does make sense. We just need to make sure that the protections are in place, that there is no risk to our security system or to any of the requirements that are—we have adopted in the House.

In the June 2017 memo outlining recommendations, there was a discussion that shared employees, both in finance and technology, do work with nongovernment-furnished equipment often at home, and that this could pose a risk to the House. I would say that that work at home is not limited to shared employees. I mean, full-time House employees do that as well.

I can think of circumstances where that would pose no risk to the House, but you identified a potential risk to the House. Could you outline what that would be and what steps we should take to mitigate those risks?

Mr. KIKO. Well, I just think any—you know, technically everybody is supposed to do work on House equipment, you know. If you are going to do work, you do use the VPN if you are supposed to communicate.

And if you don't, you are opening yourself up, your systems up to people that are trying to hack in. There is a lot of evidence of people that are trying to use these kind of systems, you know. They are trying to hack in.

Ms. LOFGREN. Well, but if I can, you know, the staff, they work weekends, they work nights.

Mr. KIKO. Right.

Ms. LOFGREN. You know, you are writing a speech, you are writing questions for the hearing tomorrow night. They are on their home computer helping to write—draft questions for you for a witness.

Mr. KIKO. I think—yeah. I mean, I think that is very difficult, obviously, to enforce, but to the extent that people can use their own House, you know, equipment to do that, it reduces the risk. That is about all I can say.

Ms. LOFGREN. Well, I guess, I don't see the risk on the policy issues that are—I mean, each Member is going to assess their risk, whether the question gets out or not is a different issue to whether our systems have been penetrated and security issues posed. Am I right, Paul?

Mr. IRVING. I absolutely agree with you. There is no question we have to differentiate between the risk the Member feels, let's say, to their data versus something that is a violation of House policy, which may not be.

But, again, if you are at home working on your home network, it is not going to be as secure as abiding by certain of our policies. But, no, you are absolutely correct. There is going to be the as-

sumption of risk there, and that may be just fine for the individual Member.

Ms. LOFGREN. All right. Thank you, Mr. Chairman for allowing me to follow up on that.

The CHAIRMAN. Thank you very much, Ms. Lofgren.

And I want to thank each of you because I know how much you all care about the institution of the House. You want it to work at the best level, and we have—certainly appreciated that hard work that you have had.

Again, I want to say thank you to the Ranking Member Brady for his work.

And all of the staff, on both sides, have—are committed to getting this right.

And I particularly, again, want to thank Mr. Davis for his continued work on this issue. It is a serious matter on how we improve the employees' safety features, let's say, particularly as it relates to the IT issues.

And while I will not discuss details of an ongoing criminal investigation, our goal is to make sure that we secure the House for the future, so that nothing like that happens again.

So with that, thank you for your attendance.

Without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward to you and ask that you answer promptly if you get them so that those answers can then be made a part of the record.

Without objection, this hearing is adjourned.

[Whereupon, at 12:20 p.m., the Committee was adjourned.]

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 11, 2018

The Honorable Gregg Harper
Chairman
Committee on House Administration
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Harper:

Thank you for the opportunity to testify before the Committee on House Administration at the Committee hearing entitled, "*Examining the Role of Shared Employees in the House.*"

Attached are the responses to the Committee's additional questions for the record. If you or your staff have any questions, please feel free to contact Salley Wood on my staff.

Again, thank you. My staff and I very much look forward to working with the Committee, its staff, and other House stakeholders this Congress in our efforts to serve the House community.

Sincerely,

Philip G. Kiko
Chief Administrative Officer

cc: The Honorable Robert A. Brady
Ranking Member

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

Response to questions for the record from the Committee on House Administration.

1. **In 2009, the Committee required shared employees to file financial disclosures. What can we learn from requiring those disclosures? Is simple filing sufficient or should we require filing and notification? How could that information help offices make better hiring decisions?**

In its 2008 special report titled, "*Controls Over Shared Employees Need Significant Improvements*," the House Inspector General (IG) recommended that shared employees, regardless of compensation, be required to file financial disclosures. In the report, the IG stated that the financial disclosure requirement would, "help the House identify potential conflicts of interest," such as the receipt of outside compensation gained through influence improperly exerted in one's official capacity, which is expressly prohibited by House Rule XXIII.

In 2009, the Committee on House Administration adopted the Shared Employee Manual that required shared employees to file financial disclosures, and, in 2012, a follow-up IG report on controls over shared employees stated that 100 percent of shared employees reviewed were compliant with the disclosure requirement.

Though there is no reason to believe that compliance with the disclosure requirement has declined, there is no data that supports or refutes whether offices are reviewing the annual disclosure submissions of their shared employees and whether such disclosure provides useful information for offices to make hiring decisions. Provided offices find the disclosures useful in making staffing decisions, adding a notification to the disclosure process would likely help.

2. **How many requests for support does HIR receive from shared technology staff and how much money does HIR spend on responding?**

Using a sample of eight of the 133 House offices that use a shared IT employee, the CAO examined 386 requests for IT support submitted in the last six months and determined that 107 – or 28 percent – of the requests fulfilled by the CAO could have been fulfilled by the shared IT staffer.

The CAO estimates the cost of fulfilling the 107 requests to be $165,000, which does not include additional costs that may be associated with the requests, including HIR management involvement, Technology Service Desk operations, Cybersecurity operations, and HIR's escalation team.

3. **How much notice do you give shared IT staff to implement necessary upgrades, modifications or changes to software or hardware?**

HIR is responsible for nearly all routine security patching throughout the House through its Secure Configuration Management Program, which patches computers remotely through the House network. For the most part, shared IT employees do not perform that work. In fact, HIR pushed nearly 200,000 patches for servers and workstations in D.C. and across the country between July and December 2017.

However, there are upgrades that do require action be taken by dedicated office IT staff, such as upgrading an entire operating system on a computer or updating the operating system on a mobile device (e.g. Android, iPhones and iPads). When office action is required, HIR seeks to provide ample notice – weeks or even months in advance, depending on the complexity of the work. For example, when offices were required to upgrade their Office 2007 suite due to the software reaching end-of-life support status, HIR communicated with offices, vendors, and shared IT employees for approximately one year before the upgrade deadline. Within the past year, HIR has decommissioned two mobile device platforms – *"Good for Enterprise" and "BlackBerry 5."* In each instance, HIR reached out to offices nine months in advance of the deadline.

Occasionally, there are urgent updates required to address known security vulnerabilities that HIR is unable to perform remotely due to lack of permissions or the inability to physically operate the devices. In those instances, HIR does its best to provide guidance and assistance to offices – virtually and in person – to quickly make the needed update. If for some reason a required update cannot be made, HIR can remove the impacted device(s) from the network so the vulnerability cannot be exploited and impact the House network. HIR understands that disconnecting a device may be very disruptive to an office and only exercises that option as a last resort.

Responses from the Sergeant at Arms to Questions from the Committee on House Administration

Questions from the Minority:

Question: In 2009, the Committee required shared employees to file financial disclosures. What can we learn from requiring those disclosures? Is simple filing sufficient or should we requiring filing and notification? How could that information help offices make better hiring decisions?

I would defer to the Clerk of the House and the Committee on Ethics for a comprehensive answer. However, from the Sergeant at Arms perspective, financial disclosures can provide additional information about the background of an individual and types of pressures to which the individual may be susceptible.

The Committee would be best positioned to determine whether filing alone, filing and notification, and what sorts of notification, if required, would best provide information to offices and the House Community.

Financial disclosures are already readily available through the Clerk's Legislative Resource Center. If the Committee elected to require notification, the type and frequency of notification should be calibrated to the purpose for which the Committee is requiring notification.

The information provided can help offices determine whether an individual is susceptible to certain types of security risks or has any conflicts of interest.

Question: One of the recurring themes of the Committee's work with shared employees is the need for background checks. You mention this throughout your testimony. As you know, there are many kinds of background checks – criminal, public trust, among others – what standard of background check should we be providing and what should we do with the results?

The Sergeant at Arms is working with the Chief Administrative Officer, consistent with Committee Resolution 115-16, to provide a plan to the Committee on House Administration within 30 days of the adoption of the resolution recommending the type of background check and the adjudication thereof.

It is likely that the type of background checks an individual undergoes will change as the House gains more experience using background checks. I anticipate it will be an iterative process. A basic criminal records history check along with a slightly more in depth former employment focused check would help improve our security process. After learning the lessons from implementing a background check process for shared employees checks and in conjunction with the CAO, more comprehensive types of background checks could be determined to be more suited for the types of risks that the House of Representatives faces.

Question: In your testimony you recommend providing shared staff a different type of ID so that the Capitol police can, quote "determine at a glance whether an individual is appropriately within an area." What do you mean by that? And could you elaborate on how providing a new badge would meaningfully reduce risk to the House?

Currently, a shared employee receives an ID from one office, but works for several offices. The shared employee is authorized to be within these other offices; however, their ID does not reflect they are authorized to be within these offices. If the USCP were checking the ID badges of all individuals within a room to see if they were authorized to be within an office, the shared employee could have a badge reflecting an incorrect office. With a shared employee badge, a Capitol Police officer is able to quickly and easily identify that further investigation is required to determine whether an employee is authorized to be within a certain office.