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

April 12, 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.