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

Before the Committee on House Administration
March 21, 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.