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

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.