TESTIMONY ON BILL 35-0086

LEGISLATURE
OF THE
UNITED STATES VIRGIN ISLANDS

OCTOBER 10, 2023

COMMITTEE ON HOMELAND SECURITY, JUSTICE AND PUBLIC SAFETY

Good day, Honorable Senator Kenneth L. Gittens, Chairman of the Committee on Homeland Security, Justice and Public Safety, other committee members and Senators present in the Chambers and virtually, other testifiers, and the viewing and listening public.

I am Kurell A. Sheridan, JD, Executive Director of the Legislature of the Virgin Islands. Today, Mr. Emmanuel "Robby" O'Neal, Director of the Management Information Systems Division, accompanies me.

I have been asked to provide testimony on Bill 35-0086. This bill seeks to amend Title 3, Virgin Islands Code, chapter 1, section 10h to require background checks for all IT personnel and employees of the Bureau of Information Technology, agencies that have data centers, and any employee who handles classified information.

I commend the bill sponsor, Senator Dwayne DeGraff, for providing the opportunity to discuss the requirement for background checks and securing information technology resources. The Legislature supports the intent of this measure. Performing a background check allows the entity to verify the information provided by the applicant or employee. The background check can also reveal information that was either mistakenly or intentionally omitted. Conducting background checks supports a safe and secure workplace and reduces risk exposure. However, it is essential to mention that this requirement, if implemented, is just one layer of protection. Additional layers implemented through policy and third-party information technology vendors will ensure that the measure's intent is upheld while ensuring a fair recruitment and employment experience for applicants and employees.

Policy

Implementing a background check requirement comes with specific policy-based responsibilities. As a government entity, we are responsible for implementing policies with sufficient procedural protections to ensure that the results of criminal background checks

are evaluated appropriately. Standard best practices for background checks are:

1. Ensuring the applicant has a chance to check the accuracy of the record before the hiring authority makes an adverse hiring decision;
2. Limiting the number of people who come in contact with the applicant's record;
3. Making sure the people who come in contact with the record are trained to read criminal records and
4. Allowing the applicant to present evidence of rehabilitation before the hiring decision.

Ensuring that a case-by-case analysis of the facts surrounding a negative background check safeguards against disqualifying qualified professionals. Factors such as length of time from the conviction and if the applicant has satisfactorily rehabilitated themselves and can be a productive member of society should be considered when making an adverse determination on an applicant or employee.

The Legislature requires that all applicants seeking employment must produce a police record from the police department both in the state or territory where the person last resided and the state or territory where the person resides. The Legislature interprets this language as an applicant who is selected for a position. Selected applicants are issued a conditional job offer, which is contingent upon satisfactory review of official records submitted (which includes a police and traffic report) and the completion of all required documents in the employment package.

The Legislature also implemented E-Verify in the 34th Legislature. E-Verify is a secure, online service that verifies an employee's authorization to work in the United States by comparing and verifying the information from the Form I-9 with records in Social Security

Administration (SSA) and Department of Homeland Security (DHS) databases.

This additional background check legislation will ensure that all persons handling classified information are thoroughly and completely vetted during the hiring or employment process.

Information Technology

Requiring background checks for employees who handle classified information is just one layer in an information security plan. Training is another layer, such as the establishment of an anti-phishing program. Training components include employee awareness and training, simulated attacks, and results analysis to guide training modifications and mitigate the risk of phishing attacks against an entity. The Legislature last conducted a simulated attack in 2022.

Third-party monitoring is another layer and is industry standard to reduce unauthorized information disclosure, threats from account impersonation, account takeover, malware, ransomware, and data loss. However, these safeguards come with a cost. Due to the rapidly changing nature of technology, the limited number of information technology professionals within the territory, and the cost/benefit of threat monitoring, funding for information security measures should be budgeted.

I thank the Senate and the public for the opportunity to discuss Bill No. 35-0086, which we support, with the policy and technology considerations outlined above. This legislation represents a forward movement towards improved information security within our government. The cost of data losses and malware attacks will far outweigh the cost of implementing background checks and further securing our data through third-party monitoring.

Before completing my testimony, I would like to thank the small but mighty Management Information Systems staff at the Legislature,

Robby, Victoria, Tafari, Pedro, and Basil, for all they do to protect this institution. Additionally, I thank Norman, Claudette, Verna, Dorothy and Migdalia, our Human Resources Team for their roles in keeping this institution safe. Both divisions play a key role in keeping systems operational so that the important work can be accomplished.

This concludes my testimony. Mr. O'Neal and I are available to answer any questions you may have.