

# Bill No. 35-0086

## 1 Title 3 VI Code, chapter 1, section 10

2 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.



PRESENTED BY

**DARYL D. JASCHEN**

**DIRECTOR**

**VIRGIN ISLANDS TERRITORIAL  
EMERGENCY MANAGEMENT AGENCY**

Submitted to

**SENATOR KENNETH L. GITTENS, CHAIRMAN**

***Senate Committee on Homeland Security, Justice & Public Safety***

Fritz E. Lawaetz Legislative Conference Room, St. Croix

October 10, 2023

3 Good morning, Senator Kenneth L. Gittens, Chairman, Committee on Homeland  
4 Security, Justice & Public Safety, other committee members, 35th Legislature Staff,  
5 and those in the viewing and listening audience.

6 I am Daryl D. Jaschen, Director of the Virgin Islands Territorial Emergency  
7 Management Agency (VITEMA). I am providing testimony today to Bill No. 35-  
8 0086, an Act amending title 3, Virgin Islands Code, chapter 1, section 10, to  
9 require background checks for all IT personnel and employees of the Bureau of  
10 Information Technology, agencies that have data centers, and any employee who  
11 handles classified information, dated May 31, 2023, sponsored by Senator Dwayne  
12 M. DeGraff.

13

14 Upon reviewing this bill, there are two concerns which I believe this committee  
15 must thoroughly be aware of and adjust language to not leave the bill vague and  
16 without substance for the VI Code.

17

18 The first is understanding the purpose of this bill as it relates to those individuals  
19 hired or working within GVI agencies, to include contractors, with elevated rights /  
20 administrative access on information technology platforms containing financial  
21 and / or Personal Identifiable Information (PII) or what would be considered  
22 insider information, which has not been released to the public through an official  
23 government source.

24

25 The second is the criteria to use to screen these Information System trusted  
26 individuals and should the “clearances” be re-validated periodically. This bill  
27 focuses on individuals who have access to information systems which are sensitive

28 in nature and if permitted to be released outside the GVI, could compromise an  
29 individual, an agency or the entire government of US Virgin Islands. The access IT  
30 workers have to sensitive information and costly equipment requires employers to  
31 have a certain level of trust and confidence in the hiring process. One bad hire can  
32 result in a significant data breach, fraud, or criminal activity that brings with it a  
33 significant amount of liability. The USVI must protect sensitive user data and  
34 disclose any data breach in a timely manner. IT pre-employment background  
35 checks help employers make efficient and effective hiring decisions by ensuring  
36 the job candidates are both competent and reliable.

37

38 A study by the RAND Corporation, published in 2021 entitled “*Updating*  
39 *Personnel Vetting and Security Clearance Guidelines for Future Generations*”  
40 found that while everyone carries some types of risks in their lives, the historical  
41 set of guidelines to assess whether these risks are low enough – based on the  
42 position to which the applicant is applying – to be acceptable to the employing  
43 agency, trends among younger adults, have shifted risk criteria to new emerging  
44 concerns. The RAND study recommended three (3) broad categories which should  
45 be scrutinized by the employer. First is with the rise of an inability to satisfy debts,  
46 student loan debts specifically, has become common for many potential applicants.  
47 Emphasis during the background check should be on management of essential  
48 debts, instead of satisfying the debts, as a risk factor. The second, is in today’s  
49 digital age, there are more opportunities to form relationships with foreign  
50 nationals through social networks for friends and acquaintances. A risk factor  
51 based on the nature of the contacts for certain countries should be examined. The  
52 third is the digital personal conduct risk involving social media platforms which  
53 could result in engaging in risky behavior ranging from illicit activities, forging

54 close personal ties with foreign and trading risky financial assets like  
55 cryptocurrencies. There should be a review of timing, frequency, and context of  
56 problematic conduct by clearance applicants.

57

58 When conducting IT background checks, it is critical for employers to follow all  
59 relevant rules and regulations. This includes provisions outlined in the Fair Credit  
60 Reporting Act (FCRA) and Title VII of the Civil Rights Act of 1964 as well as  
61 state and local laws and regulations. The FCRA states that employers must obtain  
62 written consent from job seekers before conducting any type of background check.  
63 Applicants have the right to receive a copy of any reports that are generated during  
64 the background check, and if any concerning information is uncovered, the  
65 applicant must be notified before the employer uses this information to disqualify  
66 them.

67

68 IT background checks can help screen out job applicants who have a questionable  
69 history or a criminal background. They can also verify an applicant's education,  
70 experience, and credentials, helping to ensure employers hire candidates who are  
71 truly qualified for the position. A periodic update for the background clearance is  
72 also recommended as well as a updated checks for changes in position / job which  
73 provides additional access to sensitive information.

74

75 From what I understand after reviewing this bill is that this bill should be about  
76 vetting a "trusted individual" with access to sensitive information and should not  
77 be about access to "classified information". Access to classified information  
78 implies that the organization has first, a method to classify information, usually as

79 Top Secret, Secret, Confidential, and Official and second, has the means to store  
80 the information within appropriate accredited information systems, which prevents  
81 unauthorized access, and prevents data “spillage” which is unintentionally leaked  
82 classified data from a classified system to another unclassified system through  
83 normally a common email system.

84 As to the use of the FBI’s National Crime Information Center (NCIC) to assist in  
85 background checks, this bill requires the potential employer or individual to  
86 complete the request at a reasonable cost between \$18-\$25 dollars, and I support  
87 the use of the NCIC along with a local criminal background check. The NCIC  
88 checks covers databases for Property Files, Person Files and Image Files. The  
89 NCIC database maintains seven property files. The categories in the property files  
90 includes record for articles, boats, guns, license plates, securities, vehicles and  
91 parts. The NCIC database can determine if an individual owns a piece of property  
92 or vehicle, and if that property was involved in criminal activity or if any legal  
93 actions are being taken against it. There are 11 person files in the NCIC containing  
94 the record of convicted sex offenders, foreign fugitives, identity theft, immigration  
95 violator, missing persons, protection orders, supervised release, unidentified  
96 person, U.S. secret service protective, violent gang and terrorist groups, and  
97 wanted person files. The person files are accessed most often when completing  
98 background checks. An individual may be listed in one or more of the person  
99 categories depending on what has been recorded. The NCIC background check  
100 will list all the categories where the person is found. The NCIC also stores pictures  
101 that can be returned with the background check. This picture part of the database  
102 helps to ensure that the person the background check is being completed for is in  
103 fact the person who applied for the position.

104 This bill, Bill No. 35-0086 provides a much-needed requirement for the  
105 Government of the US Virgin Islands to include measures to require background  
106 checks for any trusted information technology individuals who will have or  
107 currently have access to sensitive data to include PII. As far as I know, the GVI,  
108 including the Bureau of Information Technology, does not currently classify any of  
109 its information systems or databases but uses access control through leadership  
110 authorization for individuals with a need to know and controls levels of  
111 authorization through systems administrators with full rights. It is the vetting of these  
112 trusted individuals which the main purpose of the bill. Just as important to  
113 providing proper access to individuals to gain access to systems, it is important to  
114 remove that access when individuals move positions or leave the government. The  
115 senior official has the responsibility to notify the system administrator of changes  
116 to an individual's status.

117 VITEMA supports the basis of this bill but recommends changes to the context  
118 with emphasis on individuals with administrative rights and eliminating any  
119 reference to handling classified information or applications. Finally, while an  
120 initial background check for employment purposes is important, depending on the  
121 sensitivity of the data or vulnerability to the agency, updated checks of criminal  
122 background records should be completed on a periodic basis.

123

124 Thank you, committee chairman, Senator Kenneth L. Gittens, for the opportunity  
125 to provide testimony on Bill No. 35-0086. I am prepared to answer any questions  
126 any members of this committee may have at this time.