MINISTRY OF NATIONAL SECURITY

GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

NS: 35/27/4 Sub. XVII

August 27 , 2021

Ms. Jacqui Sampson-Meiguel
Clerk of the House
Office of the Parliament
Parliamentary Complex
Cabildo Building
St Vincent Street
PORT OF SPAIN

Ms. Sampson-Meiguel,

The Thirty-Third Report of the Public Accounts Committee on the Follow-up on the status of the implementation of the recommendations on Information and Communication Technology (ICT) governance and general controls as stated in the Reports of the Auditor General on 2017, 2018 and 2019 Public Accounts

With reference to your correspondence dated July 23, 2020 *(Ref: Parl.:5/1/2)*, pertaining to the captioned matter, please find enclosed, the information as requested by the Committee.

The late response is regretted.

Sincerely,

Mary Joseph
Permanent Secretary (Ag.)

Encl.


OFFICE OF THE PARLIAMENT
COMMITTEES
SEP 07 2021

Ministry of National Security's Response to the Recommendations contained in the 33rd Report of the Public Accounts Committee on the Follow-up on the status of the implementation of the recommendations on Information and Communication Technology (ICT) governance and general controls as stated in the Reports of the Auditor General on 2017, 2018 and 2019 Public Accounts

---

Recommendation No. (ii) (pg. 18)

The Cyber Security Incident Response Team, Ministry of National Security, should provide Parliament with its recommendation to avoid future breaches by August 30, 2020.

Response:

The Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) encountered several internal and external challenges while addressing the incident which impacted their ability to respond in a timely manner. However, to improve the cyber security posture of Government websites and to avoid future breaches, the following are recommended:-

1) **Policy - Further investigation highlighted that some of the required industry standards for cyber security controls were outdated, thereby the following should be explored:**
   i. The establishment of a Cyber Security Policy Committee for GoRTT- This can be enabled under the Government Information Technology Leadership Advisory Council (GILAC);

   ii. The development of a Government Website Security Policy - This will identify the baseline security configuration for Government websites and operational procedures;

   iii. The development of a Third Party Vendor Website Development Policy, which should outline the requirements for development, maintenance and breach notifications;

   iv. Active monitoring of all critical Government Websites through the use of a Cyber Security Monitoring Tool/System. The system should monitor up-time and downtime and identify configuration changes and vulnerabilities. This can be performed by the TT-CSIRT once the appropriate software system and human resources are deployed at the Unit;

   v. The establishment of a policy which sets the responsibility of the respective owners of the website to inform and provide cyber security incident information to the CSIRT or designated agency, inclusive of breech notification information;

   vi. The Ministry, Department or Agency (MDA) must ensure that a trained technical resource i.e. (Web Specialist/Developer) resides within the ICT Department of the MDA to monitor and manage the security configuration of the Website;

vii. All official Government of Trinidad and Tobago websites or access portals to government services should comply with a *gov.tt* domain name;

viii. A portal should be created as a validation website in order to verify the authenticity of Government of Trinidad and Tobago official websites.

ix. The Website Security Policy should include the requirement to submit a post-incident report by the entity responsible for the management of the website within fourteen days of the incident with appropriate status updates to the Ministry of Digital Transformation and the TT-CSIRT or designated Agency; and

x. All critical Government websites should be required to undergo yearly security assessments by the TT-CSIRT or have an assessment completed by a competent entity reviewed by the TT-CSIRT.

2) **Technical - Most of the websites affected were either developed and/or maintained by a third party vendor, and all of the websites were provided with website hosting by a hosting company in Miami, Florida. Therefore, the following are highly recommended to increase accountability to the Ministry, Department or Agency (MDA):-**

i. The MDA should ensure frequent updates to be applied to all elements (hardware and software) of a government website within a suitable timeframe (no more than 15-21 days after release will be considered acceptable);

ii. The MDA and the website developer or vendor are to be subscribers to the Content Management System (CMS) platform notification service, in order to be notified of update releases, patches and fixes to ensure that the website functions at the latest version of the CMS at all times;

iii. The MDA must be notified once the update has been completed via a report which outlines the specifics of the update (no more than 15-21 days after release will be considered acceptable);

iv. The MDA should be informed of any site outages such as the Content Management System (CMS), Intrusion Detection System (IDS) or any other system by the host. These outages should be reported to the MDA and the Monitoring Agency;

v. Two factor authentication must be implemented for Administrators with effective passwords;

vi. The website must be hosted with a secure reputable hosting company;

vii. A physical firewall or software firewall and website application firewall must be implemented to secure the website;

viii. Ensure all default settings on the CMS have been changed such as logins or any other default settings which can compromise the website;

ix. The website must be configured with the recommended HTTPS protocol upon deployment, and the appropriate Secure Sockets Layer (SSL) Certificate applied to the website from a reputable certificate authority;

x. Ensure frequent backups are performed to ensure the ability to recover from any incident; and

xi. Vulnerability assessments should be undertaken at regular intervals to identify risks which can affect the website.

3) Incident Response - The compromise of a government website should be minimized and response to risk should be timely to avoid such future incidents. On further investigation the following is recommended:-

i. The MDA must be notified of any attempted or successful breaches along with resolutions by the vendor, monitoring agency or incident response team within three hours of the identification of the incident;

ii. Information provided should include the type of incident (defacement, hacking, DOS, etc.) and the measures which were carried out to resolve the incident;

iii. The MDA must be notified within 3 hours of any incident which changes the public or front facing content of the website vendor or monitoring agency;

iv. The MDA is to be provided access to all logs, inclusive server and website logs in the event of an incident upon request by the authorized designate of the MDA within 48 hours of the incident by the vendor responsible for maintenance of the website or hosting provider; and

v. The MDA should be provided with regular status updates of the incident by the entity engaged in the remediation efforts, at least one update in a twenty four hour period.