Penetration Test Report

Prepared for:

Vermont Secretary of State

Prepared by:

Bilal Khan – CISSP, CCSP
Senior Solution Architect, SHI Security Services
Bilal_Khan@shi.com

1 May, 2018

Document Revision History

Document versions track changes made to this document as needed during the course of the project

Author	Version	Date	Changes
Bilal Khan	1.0	1 May, 2018	Initial version of the document. No changes.

Document Approval

A signature below indicates Vermont Secretary of State has approved of the contents of this document and final acceptance as a deliverable for the project.

Vermont Secretary of State	SHI International Corp.
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

Table of Contents

Figures

Tables

1. Executive Summary

SHI International was engaged by Vermont Secretary of State "VT SOS" to perform penetration testing during the month of April 2018. The purpose of this third-party penetration tests is to identify vulnerabilities in the computer environment where an unauthorized entity could gain access into trusted systems or information.

For the purposes of this engagement, SHI used automated and manual tests to identify weaknesses in the organization's security controls and then attempted to leverage those weaknesses to gain unauthorized access. Although artificialities were introduced to the testing process (e.g., restricted engagement vectors such as no brute force login attempts), this process sought to maximize testing efforts to measure real-world business risk to the organization's information assets.

SHI rates the overall IT security posture of **Vermont Secretary of State** considerably well established and mature in comparison to other similar organizations audited in the past annual year.

As a result of the testing process, SHI offers the following observations as the greatest risks to the organization's information and systems:

The following notable findings are provided to emphasize processes and mechanisms currently in place that contribute to the overall security posture of VT SOS.

1.1 Notable Practices

Perimeter Security Controls and Change Management Process	VT SOS has deployed a significant defense-in-depth strategy at the public Internet gateways. In general, services have been restricted on hosts that can be reached from external IPs, and SHI discovered no significant number of vulnerabilities during the testing process which indicates that the change management program successfully evaluates configurations of these hosts during their lifecycle.

As demonstrated above, significant effort is spent on maintaining the access areas into the IT infrastructure of VT SOS's environment. There are, however, areas where improvements can be made to improve or validate the security controls that are in place. These opportunities for improvement are summarized below and detailed later in the document. When evaluating these findings, they should be seen as recommendations in terms of the direction of the ongoing security effort as opposed to a single remediation action

1.2 Recommendations