US Virgin Islands Board of Elections
Elections Security Plan

1. Voting equipment Replacement and Upgrades

An assessment will be conducted of the current hardware and software to determine whether they can adequately address the needs of all stakeholders. Changes will be made to the overall system based on the results of the planned risk assessment (see item #4), the current needs of the voters of the US Virgin Islands and the available systems based on EAC certification requirement for voting systems.

Timeframe: March 2019-December 2019

2. Election Auditing (Section Not Applicable)

3. Voting Registration Systems and Management

The USVI Voter registration system will be updated so that the capabilities of the current system will be enhanced to make it more compatible with the required security upgrades. The proposed system will support a larger database since the territory's law has been changed disallowing the cancellation of voters. The new system will support the interoperability with the elections system's website that will allow voters to update their registration, support document scanning into the system, automatic check of voting eligibility, voters can check their assigned precincts and the location of their voting precinct.

Timeframe: March 2019-March 2020

4. Cyber Vulnerabilities

Considering the increasing volume and sophistication of cyber threats, the US Virgin Islands Board of Elections (USVIBOE) believe that our current physical infrastructure and voter technology systems are at great risk of being penetrated and compromised. As such the USVIBOE has decided to utilize the 2018 HAVA Security Grants funds

a) to assess and identify any potential risks
b) determine the systems cybersecurity maturity
c) Develop and implement a plan to prevent, mitigate and respond to threats or penetration.
d) Monitor and evaluate the ongoing operations

Risk Assessment

The Assessment will provide the USVIBOE and the Election System with a repeatable and measurable process of assessing and identifying our risks and cybersecurity preparedness. The Assessment will consist of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile identifies the inherent risk before implementing controls. The

Cybersecurity Maturity includes domains, assessment factors, components, and policies and procedures across five maturity levels to identify specific controls and practices that are in place.

To complete the Assessment, the system's inherent risk profile will first be assessed based on five categories:

- Technologies and Connection Types
- Delivery Channels
- Online Technology Services
- Organizational Characteristics
- External Threats

The Assessment is intended to be used primarily on a system-wide basis and when introducing new products and services as follows:

• **System-wide. Conduct a** review of the Inherent Risk Profile to understand which policies, procedures, processes, and controls are in place and should be in place system-wide and where gaps may exist. Following this review, a determination will be made of the appropriate maturity levels for the system in each domain or the target state for Cybersecurity Maturity. Management can then develop action plans for achieving the target state.

• **New products, services, or initiatives.** Using the Assessment before launching a new product, service, or initiative can help the Board of Elections and management understand how these might affect the system's inherent risk profile and resulting desired maturity levels.
The Inherent Risk Profile identifies activities, services, and products within the systems and those external connections that are needed or being utilized as part of the system.

• **Technologies and Connection Types.** Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, connections, and nature of the specific technology products or services. This category includes the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices.

• **Delivery Channels.** Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses those services that are available through online and mobile delivery channels and the interactivity of the website thus the potential for data exposure.

• **Online/Mobile Products and Technology Services.** Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. The Election system currently provide information to the public via the website. In order to ensure that the voter's information and other sensitive data is secured the website will be updated to add a more interactive, reliable, and timely feature.

• **Organizational Characteristics**. This section will consider organizational characteristics, such as number of direct employees and cybersecurity contractors, changes in security staffing or consultants, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers.

• **External Threats.** The volume and type of attacks (attempted or successful) affect the inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the system.

After completion of the assessment the system's Cybersecurity Maturity level will be evaluated for each of five domains:
• Cyber Risk Management and Oversight
• Threat Intelligence and Collaboration
• Cybersecurity Controls
• External Dependency Management
• Cyber Incident Management and Resilience

Cyber risk management and oversight.

Cyber risk management and oversight addresses the board's oversight and management's development and implementation of an effective system-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

Threat intelligence network reporting and sharing

Threat intelligence and collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties.

Cybersecurity preventative controls

Cybersecurity controls are the practices and processes used to protect assets, infrastructure, and information by strengthening the system's defensive posture through continuous, automated protection and monitoring.

External dependency management

External dependency management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the system's technology assets and information.

Cyber incident management and resiliency.

Cyber incident management includes establishing, identifying, and analyzing cyber events; prioritizing the system's containment or mitigation; and escalating information to appropriate

stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

5. Training

USVIBOE will identify and make available the appropriate training for Board, Staff and vendor personnel who has cyber risk management and oversight responsibility. Training will also be provided to persons that are identified to monitor the network, assess current and future risk, train other personnel, implement preventative controls, manage and coordinate security issues with external agencies and partners, and respond to incidents or threats.

There will also be a three-day training with all stakeholders. The objectives will be

1. to educate stakeholders on the various aspects of the US Virgin Islands Elections Security Plan, as well as updated training on the operations of old technology and any new technology that is acquired.
2. To conduct an exercise to asses the readiness of the Cyber Security Plan as well as the readiness of the appropriate personnel to manage and implement the plan before, after and during a cyber related incident.

Timeframe: July 2018-April 2022

6. Communication

Coordinate with the webmaster to upgrade our webpage to incorporate the following applications:

1. Election Official Application online
2. Election Official Quiz online
3. Application for Electors to check their status and polling place

Timeframe: January 15, 2019 – April 2022

2018 HAVA ELECTION SECURITY GRANT

Budget Information

CFDA # 90.404 — Non-Construction Program

Name of Organization: Elections System of the VI

Budget Period Start: 7/13/2018

Budget Period End: 3/23/2023

SECTION A - BUDGET SUMMARY

FEDERAL & NON-FEDERAL FUNDS (Match)

(Consolidated Budget for total project term-- up to 5 years as defined by grantee)

BUDGET CATEGORIES	PROGRAM CATEGORIES (a) Voting Equipment	(b) Election Auditing	(c) Voter Registration Systems	(d) Cyber Security	(e) Communications	(f) Other _____	(g) Other _____	TOTALS	% Fed Total
1. PERSONNEL (including fringe)			$ 40,000.00					$ 40,000.00	7%
2. EQUIPMENT	$ 200,000.00							$ 200,000.00	33%
3. SUBGRANTS- to local voting jurisdictions								$ -	
4. TRAINING	$ 100,000.00			$ 45,000.00				$ 145,000.00	24%
5. All OTHER COSTS					$ 135,000.00	$ 80,000.00		$ 215,000.00	36%
6. TOTAL DIRECT COSTS (1-6)	$ 300,000.00		$ 40,000.00	$ 45,000.00	$ 135,000.00	$ 80,000.00	$ -	$ 600,000.00	100%
7. INDIRECT COSTS (if applied)		$ -							
8. **Total Federal Budget**	$ 300,000.00	$ -				$ 80,000.00	$ -		
11. Non-Federal Match									
12. Total Program Budget		$ -		$ -		$ 80,000.00	$ -		
13. Percentage By Category	$ 0.50		$ 0.07	8%	23%	13%		100%	

Proposed State Match #DIV/0!

A. Do you have an Indirect Cost Rate Agreement approved by the Federal government or some other non-federal entity? NO

If yes, please provide the following information:

B. Period Covered by the Indirect Cost Rate Agreement (mm/dd/yyyy-mm/dd/yyy):

C. Approving Federal agency:

D. If other than Federal agency, please specify:

E. The Indirect Cost Rate is: