# Biometrics Voter Registration in Ghana: An Analysis of Gaps, Risks and Mitigation Controls

# Background

Biometric voter registration represents a means to accurately capture unique physical features of an individual in addition to demographic data of the Ghanaian voter. The intent of implementing this project is to prevent multiple voter registration and voting, as well as mitigating the incidence of voter fraud. This document aims to highlight and address gaps in the Biometric registration process as well as offer mitigation controls to limit the amount of risks that the implementation of this project presents.

Security gaps will be highlighted in the following domains: Tender process, Maintenance and Support, EC (Ghana Electoral Commissions) readiness , Storage and Physical controls applied to the Biometric data and Security requirements required of any Biometric system etc..

# Tender Process Document Gaps

Every proper IT process requires that multiple releases of product be released on a much smaller scale prior to full deployment on a larger scale. This is evidenced in what most companies do in running Alpha, Beta and Production releases of any IT product that follows proper release cycles. Systems of this scale are typically rolled out in phases and also piloted so that any technical and non-technical glitches are addressed in each phase. Biometric voter registration should have been piloted on a much smaller scale as in say a District Election or University SRC election etc... None of the afore-mentioned proper software development processes has been followed and actual implementation will be happening without any extensive testing. EC plans to implement Biometrics in less than three months, a decision that will most likely present extensive risks and glitches during the registration process.

# EC's lack of preparedness:

The EC has designated training requirements for the handling, processing, maintenance and technical support of the Biometric registration systems. Training will be offered in to 40 to 50 technicians , 3 to 5 software engineers, Data centre systems administrators and database administrators(5) , AFIS administrator (3), Adjudication Software(15)(page 66/97 of EC Biometric voter registration Tender document). On page 67, item 110 of Biometric registration tender process document, it is stated that

"Maintenance and Technical Support for the first 10 months rests solely with the supplier and it is only after 10 months that the EC is expected to have in place a technical team that can meet a sizeable portion of equipment technical problems internally." The statement above highlights EC's lack of preparedness to provide proper maintenance and support of systems associated with Biometric registration .Although EC personnel will be trained; they will rely solely on supplier for maintenance and support issues. The risk involved with this is that the registration which is a core component of this process is expected to be started and completed before the end of the year, which clearly indicates that the EC's will not have a technical team ready come registration time . In order to perform maintenance and support, the supplier will require elevated privileges on Biometric registration systems .Since supplier will have elevated access to system; the selected supplier's political tilt will matter heavily since data can be manipulated without detection.

# Data Security gaps

Multiple systems will store and process data critical to the Biometric Registration, the systems are mainly : AFIS software including adjudication functions and Servers, Voter database management software, Database Servers, Data collection software, Data storage software, Digital Mobile Voter registration kits.
At the time of enrollment, the Digital Mobile Voter Registration kit will use the voter registration software (AFIS) to register and capture voter biometric template data, this provides an avenue for users and administrators to maliciously pre-load system with already existing Biometric templates, basically perform CRUD(Create Read Update Delete) functions without detection. All >20 million Biometric Templates will be stored on the AFIS servers and will be subject to manipulation by anyone with access to system both internal/external entities. If Biometric templates are altered, user registration data will become inconsistent and thus corrupted, which will then lead to mass user rejection post-registration of valid voters.

During adjudication and review of duplicate and inconsistent voter records per (item 127,128 page 69 of EC Biometric Registration Tender document), the supervisor has the ability to change the decision made by an adjudicator and the changes logged. The questions that arise will deal with who has access to the logs and how EC intends to detect, restrict and prevent changes to log files. Additionally,

only windows based Adjudication workstations are required by Tender document to have antivirus installed whereas it is a well known fact Linux based viruses exist in the wild. There are also no requirements that will ensure that Biometric registration systems, Servers and Databases have been securely configured according to security best practices and standards.

## *Voter database Management (Data collection software and Database Servers)*

After data is captured on Digital registration kits, backups are taken on USB flash drives and data is extracted using the Data collection software. Files collected by data collection software are then loaded into voter registration database. Risk -How do you address data corruption of files from corrupted backup files, corrupted USB and corrupted Database data?

(item 149, page 72 ) deals with reports that show missing polling stations and polling stations with corrupted files, how does the EC intend to deal with these issues after registration exercise is over?(Will EC force a re-registration for affected polling station.? No controls exist to avert or sustain registration in the incidence of data corruption based on scenario above). This is a greater risk if it occurs close to Election Day and there is widespread data corruption. What data recovery methods does EC plan to implement to mitigate this risk and how many times during the course of the year will these tests be run?

How does EC plan to account for auditing, logging and monitoring of DBMS (Database Management Systems) to ensure that data user access and actions are logged? Who will have access to the auditing data and logs and what incidence management processes are in place to respond to malicious and unauthorized data manipulation of logs?

## *Voter registration gaps*

The administrative tool of voter registration software provides the following capabilities: Register and Remove Registration Officer, Registration Assistant and Data entry operator. Setup polling stations, Load polling station data, Restore polling station data. Anyone with access to such capabilities has the ability to effectively remove voters, transfer voters, edit voter data, and replace voter ID functions. There is no auditing/monitoring or logging requirement in tender process for any of these functions.

Regarding item 202, page 83 of EC Tender document, the voter data is to be encrypted using public/private key mechanism. It is technically infeasible to use asymmetric algorithms to encrypt several bytes of data due to how complex asymmetric algorithms are designed; it is typically very labor intensive thus the reason why it is used to encrypt only small blobs of data. If public/private key pairs are to be used what specific mechanism is to be implemented, what algorithms will be used, what are the key strength requirements? EC Biometric Tender process document states that each polling station will have it own key pair, in this instance, what secure key management techniques (restricting access to keys, logging and alerting on unauthorized access to keys, key splitting etc..) is the EC proposing to ensure that encryption keys do not fall into wrong hands and are properly restricted.? Access to centralized servers should be restricted and logged. All access requests for any maintenance needs to be formally reviewed and all approvals documented. Since master and provisional lists will be derived from central server, the server has to be heavily fortified, monitored and secured to prevent any breaches.

## Network, Systems and Infrastructure Security

All systems, infrastructure and networks need to be evaluated for security gaps by a reputable third-party. Although antivirus/antimalware seems to be a requirement for windows systems it is not a requirement for Linux systems. There are no requirements for all systems to be configured according to security best practice requirements and audited to ensure compliance with the states best practices. Auditing/logging and monitoring has not been called out as a requirement for all systems and no group has been assigned that responsibility. Since multiple critical files will be heavily used in this process File Integrity Monitoring (FIM) will have to be deployed to detect changes to critical system and data files. As already stated previously, every auditing/logging and monitoring capabilities needs to be reviewed by an assigned resource and all incidents need to be handling according to incident management best practices? What controls are in place for the EC to identify, detect and prevent network and systems security attacks on centralized servers?

## Physical Security Gaps

There are no identified controls to address how flash key backups will be securely transported from

polling centers to data centers. There is no mitigating control to prevent anyone from replacing the flash key backups during transport. In the incidence of data corruption of Mobile registration toolkit the USB backups will be the only available source of data and if that is stolen, destroyed or replaced during transport then voter biometric template data is lost forever. There is nothing in the tender process that details how Digital Mobile registration kits will be physically protected from theft or destruction during storage, and transport to and from the polling stations. The generators that are supplied for this exercise are expected to be protected with a simple lock (item 90,page 61/97 of EC Biometric Tender process).In an area with unreliable or non-existent power supply, how does tying a generator to tree with a simple lock address physical security concerns. With the weak physical security controls any malicious person could hold up the entire process by carrying away generator. The EC has no response plan to replace any stolen or destroyed generators with backups in an expedient fashion-per Biometric Tender process only one generator is being ordered per polling station with no backups in mind.

# Data Center Gaps

EC has not provided any guidance as to which Data Center will house the AFIS Servers, Database Servers and other systems critical to the Biometric registration process.

It is not clear as to who will be selecting the Data Center (Supplier or EC), Where the Database will be located, what certification the Data Center in question possesses (e.g. SAS70, ISO 27001/2 etc.).? The security controls required from the afore-mentioned certifications will ensure the necessary controls are addressed. What additional third-parties will have access to EC voter registration data and systems apart from Supplier? Does supplier have any defined data recovery and business continuity policies in place to address incidence of catastrophic disasters?

# Software Security Gaps

There are no requirements in the Tender process to ensure Voter Registration software and other systems are developed and configured according to OWASP/NIST/ISO 27001/27002 standards. There is no requirement that ensures that the system is configured according EAL (Evaluation Assurance Level) ratings. Supplier does not have third-party evaluation of the software, databases, infrastructure and

network. What is the CER (Crossover Error Rate) of AFIS system-the false acceptance and false rejection rates? What are the defined SLAs (Service Level Agreements) for system response times, system performance, systems security etc..?

## Certification and Accreditations:

No reputable third-party has been identified to certify that AFIS system is developed in compliance to ISO/IEC 19794-5 and ANSI/INCITS 385 standards for portrait capture and NIST, ANSI/INCITS 378 and ISO/IEC 19794-2 compliant formats for fingerprints. No reputable third-party has reviewed the physical, software, and deployment architectures of the Biometric Registration project to certify that it has accounted for any security related gaps and has certified the systems in questions as having proper security controls embedded...

## Edge Cases

There are existing gaps when it comes to addressing cases where voter fingerprints cannot be captured (people with missing fingers from injuries, diseases etc...). EC has not provided any alternatives for verifying voters in the incidence that at that they have lost their fingers at the time of voting. What options are in place to address a situation where the centralized voter registration databases crashes and cannot be recovered? How many levels of redundancies have been built into architecture to ensure that even if someone broke into data center (will backups be stored in multiple data centers to reduce such risks?) and walked away with voter registration databases there will be little to no effect on biometric registration project? What does it mean from a legal perspective if all voter registration were destroyed prior to the elections and elections had to be postponed-Does this provide an automatic extension of NDC rule.? What if party sponsored someone (arsonist) to set fire to data center if opinion polls indicated that they were on the verge of losing the elections?

## General Security Issues with Biometric systems:

There are several inherent weaknesses of Biometric systems that will need to be accounted for by the EC

in order for a system of this nature to be successfully deployed. Most of these issues are not accounted for by the EC and will leave serious security gaps in the biometric registration process. Issues that are synonymous with any biometric system are: Spoofing(using someone else's fingerprint), Sensor bypass(bypassing the sensor's ability to correctly detect user), Overwriting feature extraction(replacing captured user features with someone else's), Malicious Logging of Biometric Templates with Biometric Template Logger(BTL), Corrupting the matcher(If biometric data is corrupted, voter cannot be correctly verified), Unauthorized access to stored templates(Anyone with access to Biometric template {either legitimate| illegitimate} has the capability to delete, overwrite and corrupt data etc..), Corruption of template fetching(template fetching mechanism could be corrupted in a way that wrong data will be captured, user will not be correctly matched when it comes to verification), Decision override(adjudication decisions could still be overridden without detection , system could be tweaked to reject valid voters in either NDC or NPP strong areas)

Some countermeasures to address these concerns will be very strict and proper supervision of enrollment and verification by the various political parties, Biometric Voter registration system should have *Liveness Detection* capabilities, Template Anonymization (Encryption), Cryptography (data should be secure during transport and storage), Network Security, Database Security, Key Management, Software and Hardware should be validated to ensure that no Biometric Template Logger exists on device.

# Conclusion

Gaps exist that allow for data (biometric, biographic and demographic) to be breached within registration system and also during its transfer and storage. The system has not undergone any pilot to identify defects and flaws prior to a national rollout. Systems that store, process and transfer biometric , biographic and demographic data have very little controls to mitigate attacks .Tender process does not require any of the suppliers to have any certifications and accreditation of their systems by any reputable third-party security firms to ensure that security best practices are adhered to. There is also no third-party certification requirement that supplier AFIS systems are compliant with ISO/ANSI and NIST standards.

There are several gaps in the tender process and implementation that will have to be resolved prior to rolling out Biometric voter registration. There should be monthly requests for Master lists for various

polling stations to ensure that users have not been added maliciously. The entire registration process should be videotaped and registrants cross-checked with Master list details. All adjudications should have representative from all parties present and needs to be recorded as well. Although authentication (two step process of identification and verification) is the major reason for using any biometric system, verification will fail if the gaps presented in this paper are not addressed. If Biometric data is manipulated, massive voter rejection will occur since valid voters will fail verification. As observed and highlighted in this document, the processes is fraught with gaps and it is my fear that there is not enough time to properly address these concerns before rollout. It is my recommendation that this Biometric voting be avoided until all the stated issues have been addressed.

## The Technical Case

### 1. General

1.1 The use of AFIS biometrics (for registering eligible voters) should be considered as a tool and not the goal of achieving a credible Voters Register and subsequently an accurate count on voting day. The use AFIS biometrics is not a panacea for all the ills and eradication of electoral fraudulent practices and must therefore be subject to comparable scrutiny as with current technology - photographs and manual registration.

1.2. It is possible for stakeholders now to authenticate the photographs and the manual method of registration done by the EC, thus it must be made possible for stakeholders to authenticate the proposed IT based AFIS system. Stakeholders must engage the services of agents to confirm the accuracy of the compilation of an entirely new voter data-base that includes biometric data captured by the EC. The integrity of the current system is based on transparency of the manual system. The proposed system should have comparable transparency - auditable and verifiable.

1.3 Breaches in the current system are as the result of failures of stakeholders to audit data. The proposed system however has inadvertently built-in avenues for deception without detection.

### 2. Unsuitable Technology – AFIS & Certification

2.1 Contrary to international best practice, the RFP does not demand an AFIS Biometric Search Engine, which is central to the whole re-registration exercise. Rather the description for an AFIS enhancer that presupposes that the existence of a biometric database that will be ‘cleaned-up’ / enhanced. It is impossible to enhance anything data to a state better than the original.

2.2 Inadequate Technology - Hardware (fingerprint scanner and camera)The creation of a demographic and biometric database a as deliverable is absent in the RFP. The document only specified an AFIS database management system. The Electoral Commission has not specified in the RFP that a reputable recognized international third-party should certify that AFIS system developed for biometric registration is in compliance with ISO/IEC 19794-2 and ANSI/INCITS 385 standards for portrait capture and NIST, ANSI/INCITS 378 and ISO/IEC 19794-2 compliant formats for fingerprint.

**3. Inappropriate Technology -Software**

3.1 Any system of this sort must operate on a web-based server as there are different components, functionalities and oftentimes-conflicting performance demands on the entire system. The entire solution on any MRW or fixed workstation may be inoperable if any application fails. Thereby rendering the whole system to crash.

3.2 There are no requirements in the Tender process to ensure Voter Registration software and other systems are developed and configured according to OWASP/NIST/ISO 27001/27002 standards. There is no requirement that ensures that the system is configured according EAL (Evaluation Assurance Level) ratings. Supplier does not have third-party evaluation of the software, databases, infrastructure and network.

3.3 The training of 3 to 5 software engineers on voter registration software AFIS system, and source code delivery may lead to the abuse of the security and functioning of the software. This will give unauthorized access and changes to the software with without log/record/register of modifications. We suggest that either all stakeholders have access to the source-codes or they are proprietary to the extent that any single unit or technical expert with access cannot compromise the functioning of the solution.

3.4 All key stakeholders should be setup to monitor all the changes to the software. Having a supplier in this instance providing the source codes of any system suggests that there will either be operational (in-auditable or verifiable) modification to the system or there is an attempt to own the intellectual rights to the software. The ability to modify without detection is an undesirable request.

**4. Inadequate Technology - Hardware (fingerprint scanner and camera)**

4.1 Fingerprint scanners should have 1200 dpi resolution to get sufficient fingerprint minutiae as against 500dpi specified by the RFP to accurate biometric data for analysis.

4.2 The use of a 2 mega-pixel webcam for the capture of voters' facial images is infant webcam technology and is incapable of being used either for facial biometric capture and storage or adjudication in case of an AFIS hit.

Digital images of faces taken with superior mega-pixel cameras (10 mega-pixel), under laboratory conditions cannot achieve an accuracy level of 50%. Under variable field conditions the accuracy of a 2 mega-pixel camera should not be expected to achieve any more than 30% accuracy. Such an accuracy level being used as a secondary and back-up method adjudication is prone to massive abuse and inaccurate adjudication.

**5. Physical Security Gaps**

5.1 Flash drives, memory stick, and all portable data storage devices should be discouraged as they permit un-authorized manipulation of data from work-stations that have already been described as storing the data of voters - rolling basis for registration). Recommended international best practice is to have a secure encrypted transfer protocols for all data transfer without the use of portable storage devices (pen drives).

5.2 Given that there may be the usage of portable storage devices, there are no identified controls in the RFP to address these cure transportation of data from polling centers to the data centers. There is no mitigating control to prevent anyone from replacing the portable devices during transportation.

5.3 In the incidence of data corruption of Mobile registration toolkit the USB backups are being specified as back-ups will be the only available source of data and if stolen, destroyed or replaced then the Voters Register including biometric template erroneous.

5.4 There is nothing in the tender process that details how Digital Mobile registration kits and the data therein will be physically protected from theft or destruction to and from the polling stations.

**6. Data Center Gaps**

6.1 EC has not provided any guidance as to which Data Center will house the AFIS Servers, Database Servers and other systems critical to the Biometric registration process. It is not clear as to who will be selecting the Data Center (Supplier or EC), Where the Database will be located, what certification the Data Center in question possesses (e.g. SAS70, ISO 27001/2 etc.)? The security controls required from the afore-mentioned certifications will ensure that the necessary controls are addressed. The RFP has not defined data recovery, redundancy or business continuity policies in place to address the incidence of catastrophic disasters.

**7. Additional Security Gaps**

7.1 General Security Issues with Biometric systems: There are several Inherent weaknesses of Biometric systems that will need to be accounted for by the EC in order for a system of this nature to be successfully deployed. Most of these issues are not accounted for by the EC and will leave serious security gaps in the biometric registration process. Issues that are synonymous with any biometric system are using someone else's fingerprint, bypassing the sensor's ability to correctly detect user, replacing captured user features with someone else's, corrupting the matcher, unauthorized access to stored templates(Anyone with access to Biometric template {either legitimate| illegitimate} has the capability to delete, overwrite and corrupt data etc.), corruption of template fetching (template fetching mechanism could be corrupted in a way that wrong data will be captured, user will not be correctly matched when it comes to verification). Decision override by an adjudication decisions could still be overridden without detection.