NIGERIAN COMMUNICATIONS COMMISSION

Strategy for Addressing National e-Governance Risk

Olusegun H. Olugbile

Vice Chair –Technical Working Group

Nigerian Child Online Protection Strategy

www.cop.gov.ng

Vice President | Member of the Board of Directors

GLOBAL NETWORK FOR CYBERSOLUTION LTD/Gte

Cybersecurity advocacy & e-Crime Countermeasures

www.cybersolutionafrica.org

Introduction|
E-Governance - a new digital innovation in the electronic delivery of public services and information between the government and the citizens.

However, the tremendous capabilities of e-governance is threaten due to the risk factors inherent in the current e-governance system .

Most Unfortunate |

e-governance (e-G) risk exposure and assessment from Cybersecurity point of view receives little or no attention in the handlers of e-governance projects in the country.

Cybersecurity of critical components of e-governance infrastructure is an extremely urgent subject matter worldwide.

The Objectives of the Presentation

1. To highlight the cybersecurity risk and structural weakness of e-governance, the root cause and the impact on the e-governance

2. To provoke strategic needs for structural re-adjustment through fundamental engagement of the framework of Cybersecurity strategy.

E-Governance (e-G) | What is it about?

- A deployment of internet for delivery of government information, and services to the citizens - (United Nation 2006; AOEMA, 2005).

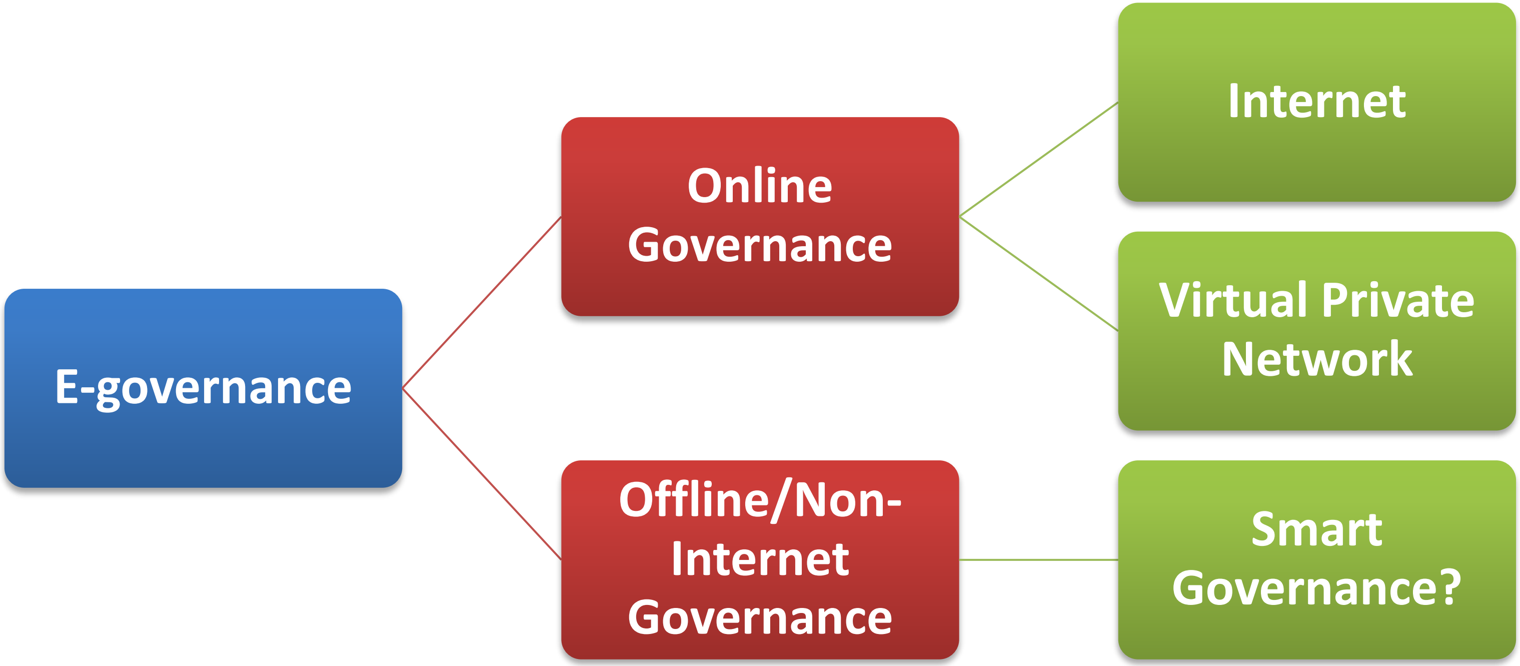
- **Involve the use of information and communications technologies (ICT) by governments to enhance the range and quality of information and services provided to citizens, businesses, civil society organizations, and other government agencies in an efficient, cost-effective and convenient manner, making government processes more transparent and accountable and strengthening democracy.**

- The World Bank Report

The e-G demonstrate applications of ICT to facilitate the operation and the disbursement of government information and service delivery. It therefore, rely heavily on the internetwork of ICT infrastructures, internet and non-internet applications to aid the operations of government.

(Jeong 2007).

2 Main Categories of e-G



E-governance

Online Governance

Offline/Non-Internet Governance

Internet

Virtual Private Network

Smart Governance?

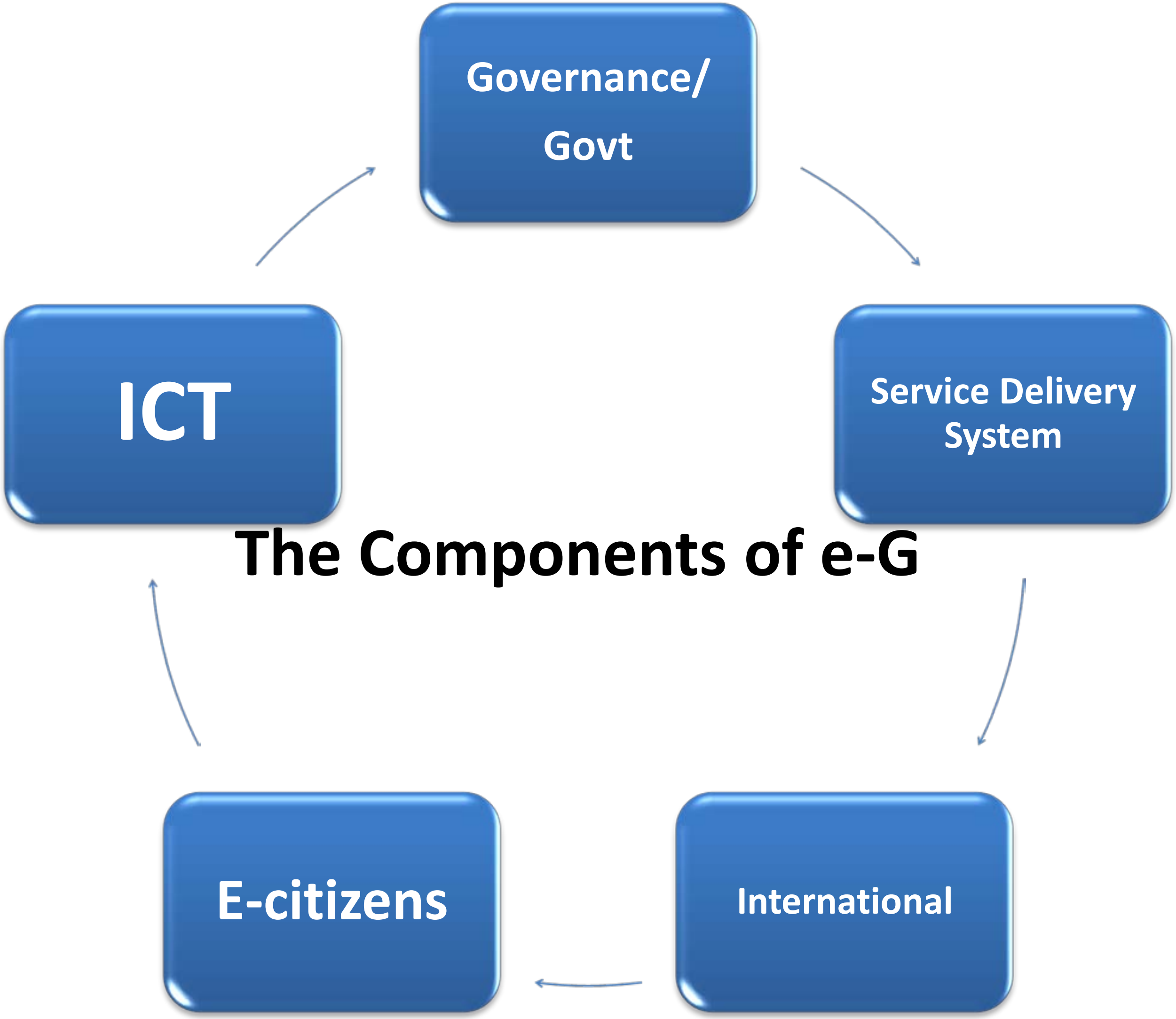
e-G means e-governance or e-government

Operational Scope of e-G

Traditionally, e-G is centered around the operations of government

Currently, e-G now include citizen engagement and participation in governance through the use of ICT to achieve better governance.

The Components of e-G



Governance/

Govt

Service Delivery System

International

E-citizens

ICT

Mode of e-G delivery & their Limitations

1. **Government to Citizens (G2C)**

   Uses CRM principles, where citizen is seen as customers or consumer. E.g Nigerian Immigration Portal

2. **Government to Business (G2B)**

   Government transaction dealing with contractors/organize private sectors. E.g Nigeria Stock Exchange Portal, CBN portals, e-payment system

3. **Government to Employees (G2E)**

   E.g Nigeria Pension Scheme System,

4. **Government to Government (G2G**)

   e.g Unified Communication via a structure dedicated Virtual Private Network. Usually among heads of state.

Strategic Importance of e-G

i. Facilitate faster disseminations of government information
ii. Allow users to engage in real life feedback dialogue
iii. Simply government transaction process
iv. Transform citizen into an active participant in governance
v. Reduce cost of governance via elimination of physical barrier
vi. Simplify the process of governance

Outcome of E-Governance

From Government Perspective

It **transform** the entire relationship between the public sector and users of public sector through a creative utilization of Electronic delivery system, in a way that strengthen a nation and grow the economy immeasurably in more transparent, cost effective and premeditated way.
- UNPNA

How far have we been able to achieve this outcome?

Where is Nigeria’s position?

United Nation Public Administration Network’s Global e-Governance Readiness Index

The Verdict: No African country listed among the top 50 countries – UN’s 2010 e-Government Readiness Index.

The United Nations Public Administration Network conducts a bi-annual e-G survey 191 member states including Nigeria based on two main indicators;

State of e-government readiness based website assessment, telecommunication infrastructure and human development and Extent of e-participation.

From Cybersecurity Perspective

To achieve a **trusted e-services** built and driven on the core principles;

- **Confidentiality**
- **Integrity,** and
- **Availability (CIA)**

How far have we been able to achieve this outcome? Basis of Evaluation? No Comment!

Trusted E-Governance Delivery Strategy - Critical Success Factors

- To achieve a **trusted e-services**, e-Governance strategy needs to focus on the central principles of Cybersecurity’s CIA.

-Effective information security measures that will limit the e-G risk exposure need to be integrated at the foundation level of e-G design and development, and implemented harmoniously throughout the operational

The E-G Security Risk

The E-G Security Risk

1.Complexity of threat

From Information security perspective, threat is any activity that can cause possible danger to the resources, information, data, and operation of e-G system in a manner that would affect the confidentiality, integrity or availability of e-services delivery or system.

E-Governance Risk Exposure

Types of E-G Threat	Nature Threat	Ultimate Goal	Mitigation Strategy
High Risk Threats	• Well-resourced, highly-motivated groups of cyber-warriors who are both aggressive and pervasive. • Numerous attack vectors including email, social media, and apparent trust paths like those with contractor facilities • Use of zero-day attacks and exploitation of weak credentials are common • Often referred to as the Advanced Persistent Threat in public media • Can be internal or externally perpetuated • Infrastructural/natural disasters either by the nature or man made	Attack of national Economy /security Political propaganda Industry espionages Intellectual property Backdoor Activitism (E.g wikileak)	National Cybersecurity Readiness & Response Strategy Covering the following 5 measures □ Technical □ Local Expertise □ National Structures □ Legal □ High-net worth awareness

Types of E-G Threat	Nature Threat	Ultimate Goal	Mitigation Strategy
Medium Risk Threats	• Criminals targeting identity and money • Varying levels of technical sophistication • Botnets and Bot Herders • Usually externally perpetuated	Target individuals or entities, usually for criminal purposes like stealing someone’s identity and ultimately their money Target agnostic towards Federal government or private company Individuals and groups of varying technical	Strong enforcement of industry best practices will help significantly with stopping both Low and Medium Risk Threats
Low Risk Threats	• Standard Internet Pollution/intruders/irritants • Threats against every user • Unsophisticated but tactical • Technical in nature – worms, viruses, script kiddie hackers • Can be internal or externally perpetuated	Nuisance variety - do not target specific individuals or entities for any specific purpose	

2. High level vulnerability of e-G network.

From Information security perspective |

A structural weakness cause by critical flaws or errors of technical oversight usually during the design , development, implementation or configuration of e-G system which could be externally or internally exploited by a threat.

What is e-G Vulnerability?

- Risk exposure is determined where there are existence of threats and vulnerability.
- In e-G, system vulnerabilities are the main doors through which threat can manifest.
- **The major worries of Information Security is not the threat to the e-G, but the massive vulnerabilities of e-G structural component, e.g software flaws, inferior substandard ICT hardware, poor configurations of mission critical system, unregulated policies, etc.**
- **E-G vulnerability are usually hidden and undiscovered**
- **Most unfortunately attacker or criminal are usually smarter than e-G planners. Why? Because they discovered vulnerability faster and long before the e-G planners discover them**

Why Are We Concerned About Cyber Security?

Our Country cyber landscape is electronically porous, structurally uncoordinated, unprepared and exposed!

On the internet, either online or offline, we are like a structurally exposed glass house with weaken frameworks, and porous windows and doors, with gullible occupants operating within a highly vulnerable environment.

1. National Cybersecurity Policy:

A renewable national statement of policy on safety and security of our engagement in cyberspace. **The policy must be captured within the emerging ICT policy. Or driven through a new legislation**. It provide basis for National Regulation, compliance and satutory empowerment to address e-G Risk.

2. Cybersecurity Governance bill.

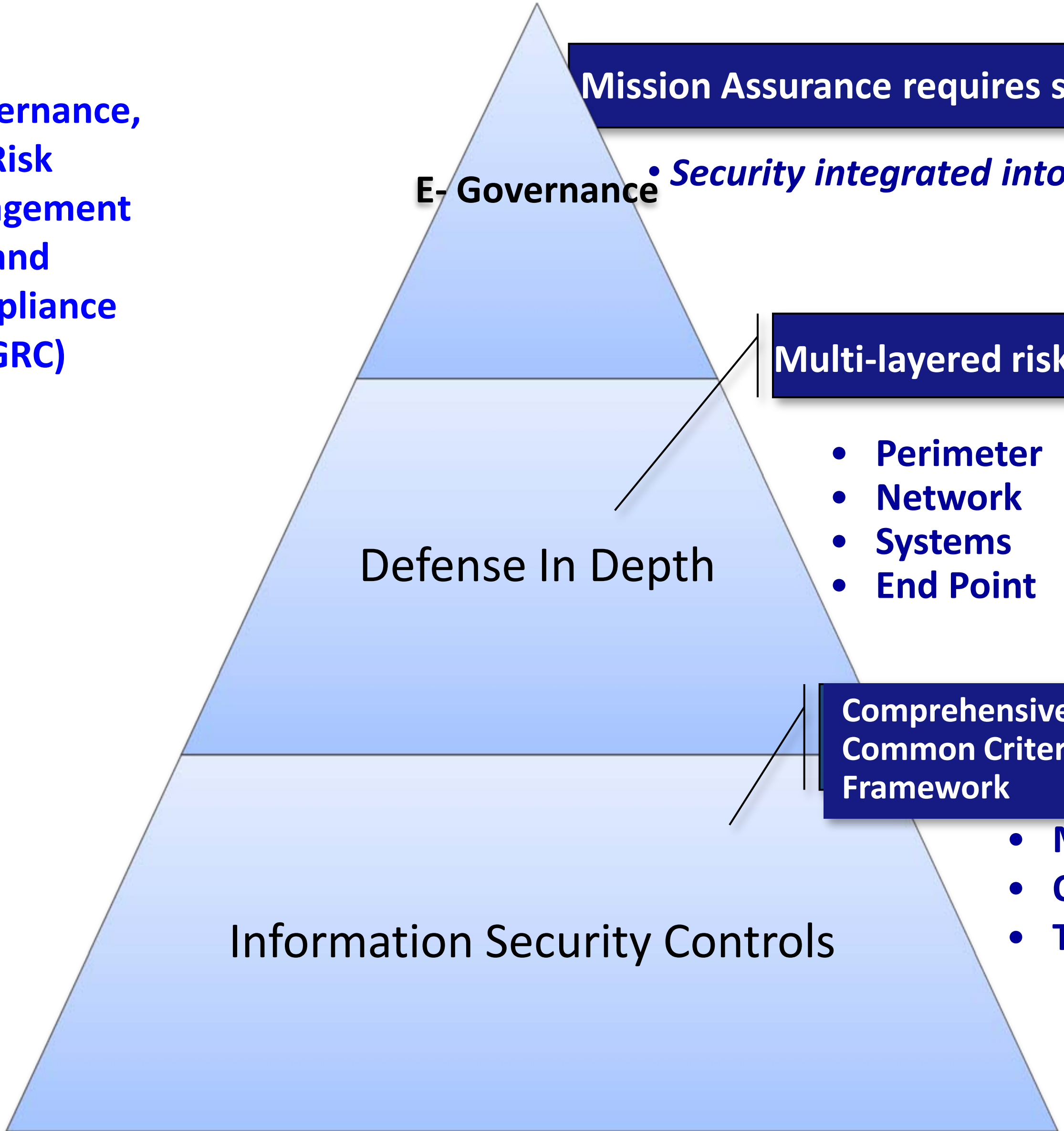
This will require the Executive and lawmaker's strategic understanding and cooperation for its actualization. **This *law*** will translate Nigeria well articulated local National cybersecurity policy into action plan for the country. **The law will protect and safe-guard Nigerian people, economy and socio-political institutions and interactions within the global domain of cyberspace**. **It will provided foundation for the digital Nigeria to operate seamlessly and compete favorably and competitively in the cyberspace.**

3. Development local Expertise in Cybersecurity

Our ability to protect ourselves and to resist exploitation of our vulnerability is ultimately depend on our diverse youth and young people that have found new way of life in cybercrime and cybersecurity.

Information Security Transformation Model For E-G Strategy

E-Governance,
Risk
Management
and
Compliance
(GRC)



E- Governance

Mission Assurance requires strong IT Security framework

- *Security integrated into IT GRC Framework*

Defense In Depth

Multi-layered risk mitigation strategy

- Perimeter
- Network
- Systems
- End Point
- Information & Data
- Security Operations
- Identity Management
- Training & Awareness

Information Security Controls

Comprehensive controls based on National Common Criteria on Risk Management Framework

- Management controls
- Operational controls
- Technical controls

Regulatory Framework focusing on E-G Defense-in-Depth

Links in the Security Chain: Management, Operational, and Technical Controls

- Risk Assessment
- Security planning, policies, procedures
- Configuration management and control
- Contingency planning
- Incident Response planning
- Security awareness and training
- Security in acquisition
- Physical security
- Personnel security
- Security assessments and authorization
- Continuous Monitoring

- Access control mechanisms
- Identification & authentication mechanisms
- (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Boundary and network protection devices
- (Firewalls, guards, routers, gateways)
- Intrusion protection/detection systems
- Security configuration settings
- Anti-viral, anti-spyware, anti-spam software
- Smart cards

Adversaries attack the weakest link…where is ours?

Strategy to address e-governance risk (Cntd)

1. National e-Governance system deployment requires strong IT governance
   Integrating core principles of information security into National e-G framework National Cybersecurity Strategy via 5-framework approach; Technical
2. Instances of Cybersecurity measures that address E-G Risk IOC Case study: National Capacity Building – IOC
3. PKI case study: securing National e-governance communication
4. Honeypot case study: Building e-security counter measure against external threat.
5. Compliance Case study: Industry ISO Standards Vs Govt Regulation

National Cyber Security Strategy
Time to Move!

From	To
IT Security in Cylinders of Excellence	IT Centers of Excellence – Building an integrated, enterprise focused IT Security Program
Capability-Focused Operational Awareness	Real-time Federated Operational awareness of threats, vulnerabilities and assets (automated and manual)
Limited Compliance	Full Compliance (crawl, walk, run)
Limited Data Protection	Full protection of systems and data commensurate with mission needs and information security levels

Thank you