Contribution ID: **17** Type: **Interactive Content Presentation**

Secure Digital Asset Techniques

Introduction:
Nuclear security is the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, or other radioactive material, associated facilities, or associated activities. As the uses of computers grow, so also the target space that criminals will try to manipulate either as tools for attack or as objects of attack themselves.
United States (US) National Institute for Standards and Technology (NIST) framework prescribe that one should 'develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services' .
Sensitive Digital Assts (SDAs) are sensitive information assets that are computer-based systems and need computer security measures for their protection. SDAs provide support systems for nuclear safety, nuclear security, nuclear material accountancy and control functions, store and process sensitive information related to such functions.
SDA is one for which if compromised, exploited, or failed, could impact the functions of the nuclear facility. The compromise of their confidentiality, integrity or availability (CIA) could lead to:
1. Unacceptable radiological consequences,
2. Theft of nuclear material,
3. Loss of sensitive information, or
4. A degraded capacity to prevent, detect and respond to a nuclear security event.
Digital Assets all have one or more of the following characteristics;
• They are of (high) value to the organisation.
• They are not easily replaceable without cost, skill, time, resources or a combination of all as the case may be.
• The loss or compromise of their CIA threatens the Organization's functionality and prestige.
• They form part of the organization's corporate identity.
• Their data classification would normally be proprietary, legal, highly confidential or top secret.

You cannot protect the devices that you cannot see or know anything about. One of the most important requirements is that organisations identify their SDAs support systems that perform nuclear safety, nuclear security or nuclear material accountancy and control functions, or that store and process sensitive information related to such function. Clearly understand the organisation's digital assets, including:
• Where the assets are physically located and their functions in the network.
• The network connectivity and information flow.
• The consequences of any combination of loss of CIA on these assets.
Securing the SDAs is an attempt to describe the protection of a very complex and expanding set of programmable electronic devices and their supporting architecture; ranging from main frame computers to programmable logic controllers (PLCs) with applications from nuclear power plant safety systems to physical security monitoring systems.
The objectives of the SDA Design Techniques are to,
1. Prevent –Stop unauthorized access to SDAs.
2. Detect –Tracking authorized user's activities.
3. Response –Minimize, mitigate effects and aid timely recovery.
Designing security techniques requires a risk informed approach i.e. you know what the threat vectors, the likely causal agents are. The design techniques should meet certain requirements and possess certain characteristics. Efforts are made to ensure that the SDA techniques do not risk causing spurious or incorrect actions that could lead to plant trips, plant equipment damage, or worse, accident conditions.
Design Techniques:
Digital Assets are diverse and there is no one protection solution or design technique fits-all. However, there are certain design techniques that are invaluable in securing our SDAs, such as; Design Basis Threat (DBT), Ruggedized Devices, Graded Approach, Defense in Depth, SDA Hardening, Physical Protection, Detection, Delay and Monitoring Capability, Penetration Testing, Regulatory/Industrial Compliance and Incident response, to mention but a few.

Gender

Male

State

Nigeria

Author: Mr OCHEME, Innocent (Nigeria Atomic Energy Commission (NAEC))

Presenter: Mr OCHEME, Innocent (Nigeria Atomic Energy Commission (NAEC))

Track Classification: CC: Information and computer security considerations for nuclear security