World Health Organization
Representative Office for Viet Nam

Call for Expressions of Interest and Proposal

#041 – Job Title: To assess the electronic non-communicable diseases (NCD) reporting system for safety as requested by the Government according to Decree number 85/2016/ND-CP on the security of information system.

1. Background

NCD management, especially at commune health stations is critical to reduce huge treatment gap and it's one of the first priorities in Viet Nam. Reporting on NCD management is to monitor outcomes of patients and coverage of the services. The result from reporting is for decision making to improve quality and coverage of the service. It is also for evaluation of NCD management program.

To have good system for reporting on NCD management, the Electronic Health Administration (EHA), MOH got support from the WHO to develop NCD software based on DHIS2 in 2021. This software works as an electronic NCD reporting system and went to operation since middle of July 2021. As of 31 August 2022, there are more than 2,700 commune health stations (CHSs) in 50 provinces using the software to generate real time report on NCD management. Data on hypertension and diabetes management have been automatically transferred from the software into the national health statistics software to reduce the workload for health workers.

In order to meet with the government's requirements on information security inspections and assessment pursuant to Decree number 85/2016/ND-CP on the security of information system by classification, the EHA of MoH requested WHO's support for consultancy for assessment of security of the electronic NCD reporting system.

2. Planned timelines

Start date: 01 Nov 2022
End date: 20 Dec 2022

3. Work to be performed

a. Check application for information security weaknesses

Tasks that need to be inspected and assessed for information security of portals/websites, & information technology services at the units under the Ministry of Health (MoH):

- Gather information on systems; develop implementation plans and measures to limit risks.
- Check for unauthorized execution of program codes
- Check for Injection Vulnerabilities
- Check for authentication errors and bypassing authentication (Broken Authentication)
- Check for sensitive data exposure
- Application attacks that handle XML data (XML External Entities) and Cross-site request forgery (CSRF)
- Check for broken access control and unsafe direct object reference error (Insecure Direct Object Reference)
- Check for security configuration errors (Security Misconfiguration)

- Check for XSS (Cross-Site Scripting) and the use of FCK Editor for information security vulnerabilities
- Checking for Insecure Deserialization and Buffer Overflow
- Checking for library errors (Using Components with known vulnerabilities)
- Insufficient logging and monitoring error checking
- Check for server request forgery (Server-Side Request Forgery)
- Check for design errors (Insecure Design)
- Check for Software and Data Integrity Failures, and vulnerabilities in the use of cryptographic algorithms (Cryptographic Failures)

Synthesize reports, analyze test results, evaluate, and instruct on fixing the detected vulnerabilities

b. Check Servers for information security weaknesses

Evaluate server information security

- Inspect system update status
- Inspect services on the system
  - Inspect the default running services of the system
  - Inspect the currently active Network Service
  - Inspect iptables service
- Inspect system management policies
  - Permissions on the system's password files
  - Permissions of user role and files on the system
  - Inspect Password Policy that is currently applied on the system
- The system access policy

Inspect the existing users on the system

  - Sudo configuration
  - Last login
  - Inspect SSH configuration
- Weakness detection: using vulnerability scanning tools, analysis and identification process in order to find, detect and identify some typical weaknesses:
- Weaknesses on the application platform: old applications, containing dangerous weaknesses (Example: Heart Bleed...)
- Weaknesses on running service instances: old version, contains vulnerabilities
- Weaknesses related to OS patches and hotfixes
- Password weaknesses: Not setting authentication passwords, weak passwords that are easy to guess
- Attacking and exploiting security holes: From the weaknesses identified from the above step, experts conduct a test attack to:
- Prove the existence of a weakness.
- Provide Proof of Evidence.

c. Check and evaluate information security of databases

Check that the databases' security patches are up to date, & what security flaws can be caused by these missing patches.

- Check on the configuration of decentralized settings for users and DB_LINK, JOBS (if any) on the system of databases according to the Security Guidelines Standards.
- Check on databases' configuration parameters against security standards:
  - Check the configuration of databases management systems

- Check the Access Control to the Service of DBMSs
- Check the configuration and archive the audit log.

- Check the user's password policy in the system, the strength and weakness of the password.
- Check the availability and forms of support and recovery when there is a problem that disrupts the system and loses data.
- Check the integrity of SYSTEM objects on databases.
- Check data penetration:
  - Test the attack scenarios against published bugs (CVEs) of the current DB version such as:

  o Intrusive attack against databases (DB listener attack, Database remote services attack, SQL Injection error attack)

  o Databases Privilege Escalation Attack: Escalates privileges to a user with higher privileges in the databases.

  - Detect backdoors, rootkits on the system

  o Check the system for backdoor or rootkit.

  o Install backdoor for the databases – affect the databases' log (Implement the installation of backdoors for the purpose of testing system hacking).

Specific deliverables:

Submission of reports of the assessment with recommendations to reduce the risks (if any).

4. Specific requirements:

a. Service provider

Service provider must be **an institute** that has License to trade cyberinformation security products and services, granted by an authorization unit.

The vendor must have used a vulnerability, malware and monitoring tool that is developed, copyrighted and owned by a local business.

b. Personnel

Request personnel to participate in the service implementation

Administration:

Quantity: at least 01 staff

Qualification

- University degree in Information Technology or Electronics and Telecommunications
- 3 years of experience and 03 projects in a similar position.

Technical Team Leader:

Quantity: 01 staff

Qualification:

- University degree in Information Technology or Electronics and Telecommunications
- Have at least 2 of the following international security certifications: OSCE (Offensive Security Certified Expert), OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), CISSP (Certified Information System Security Professional), CHFI (Computer) Hacking Forensic Investigator), CSPA (CREST Practitioner Security Analyst) or equivalent.

Experience: Minimum 10 years of experience and 01 equivalent project.

Staff involved in project implementation:

Quantity: at least 03 staff

Qualification

- University degree in Information Technology or Electronics and Telecommunications
- There is at least 1 staff with at least one of the following certificates: OSCE (Offensive Security Certified Expert), OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), CISSP (Certified Information System Security Professional), OSWE (Offensive Security Web Expert) or equivalent.

Experience: Minimum 03 years of experience and 01 equivalent project

5. Place of assignment:

- In Hanoi and the workplace of the service provider.

6. Travel

- Travel in Hanoi and to other provinces depending on requirement.

Those who are interested can submit your most updated CV and application letter indicating post title and vacancy notice number ***by 10 October 2022*** and should be addressed to:

Administrative Officer
World Health Organization
UN Building, 304 Kim Ma Street,
Hanoi, Viet Nam

OR
wpvnmapplicants@who.int

For further information on this TOR, please contact:
wpvnmwr@who.int