National Center for Mental Health
Nueve de Pebrero St., Mauway, Mandaluyong City

Integrated Hospital Operations Management Program / Information Technology Unit

Terms Of Reference

Deploying, Commissioning, and Configuring of NCMH Endpoint Security

I. BACKGROUND

National Center for Mental Health (NCMH) is undergoing digital transformation to satisfy requirements in becoming the premier training and research center for the development of interventions on mental and neurological services in the country in accordance with the IRR of the RA 11036 also known as Mental Health Act. To implement expanded services and mandate, NCMH had embarked on digital transformation and ICT modernization initiatives for its institution. These will have an impact on every component of current hospital processes, programs, and strategies, resulting in increased accessibility, reduced inequality, and increased patient knowledge, paving the way for more opportunities to service users for better promotive and preventive care (Blix & Levay, 2018).

Unfortunately, as modernization and digitalization rise, incidents involving cybercrimes and attacks also increase. As institutions innovate to technology-dependent entities, cybersecurity becomes a vital part of the digital transformation of an institution. Newer techniques and strategies are introduced when implementing digital as its exploits. There are growing concerns in GHS that cybersecurity in healthcare is insufficient and is already resulting in a loss of confidentiality and integrity of data (Coventry & Branley, 2018). In 2016 alone, Symantec detected 1 million new malwares created daily (Symantec, 2016). Globally, healthcare was struck by cyber-attacks that resulted in economic breakdowns, loss of reputation and trust, and lawsuits. Incidents in the healthcare industry related to cyber-attacks hit an all-time high in 2021 and exposed the Personal Health information of 45 million individuals. It has increased by 32% from the previous year (Landi, 2022). It was also revealed that 70% of the hospitals globally had experienced a relevant cyber security incident in the last twelve months that disrupted IT operations, business functions, data breaches, and financial losses (2020 HIMSS Cybersecurity Survey). In fact, in Kaspersky's event called Cyber Security Weekend 2019, held in Yangon, Myanmar, Yury Namestnikov, head of the global research and analysis team for global cybersecurity research firm Kaspersky (Chua K., 2019), revealed that 76% of the medical devices in the Philippines are infected with malicious code. It includes tablets, hospital machines, and servers that cater to Personal Health Information.

Cyber-attack incidents became rampant because healthcare facilities were not ready enough for the consequences of digitalization. They did not expect the digital risks and their resulting events might bring their institution to its knees. No dedicated staffing, lack of budget, and prioritization, thus resulting in poor cybersecurity posture. One of the most significant reasons cyberattacks are successful is that attacks are not monitored and detected continuously. IBM revealed that the average time to detect a breach by an institution is 200 days (Ponemone Institute 2016). 75% of leading cybersecurity providers revealed that monitoring and detection are much more difficult nowadays because cybercriminals keep developing newer and more advanced techniques and procedures to evade perimeter security tools (Symantec, 2019). It was also revealed that 66% of the institutions agreed that threat monitoring is limited because the tools are independent. Additionally, 64% agreed that their efforts in monitoring are hindered because it utilizes too many manual processes (ESG 2019).

II. OBJECTIVES

1. **Preserved Confidentiality, Integrity, and Availability (CIA) while having an economic and cost-saving cybersecurity implementation** - Rapid and exponential modernization and digitalization in Government Health Sector (GHS) enabled it to become evidence-based, economical, and timely but this introduces a greater risk of threats, exploits, and vulnerabilities. The implementation of digital solutions such as Electronic Health Records (EHR), Electronic Medical Records (EMR), Telemedicine, and the Internet of Medical Things (IoMT) has made cybersecurity a critical aspect of healthcare technology infrastructure (Jalali, M. et.al., 2019). Healthcare has become more reliant on digital solutions now than ever and because of this, according to Alharam and El-madany (2017), the healthcare industry became the most attacked by criminals. It was recorded that a total of 100 million Personal

Health Information (PHI) was successfully breached across 100 different countries. This caused business disruption, compromised health information, and risked the safety of the service users involved (Ghafur S., Grass, E. et.al., 2019) Successful attacks can cause not only technical effects but also nontechnical issues such as lawsuits (these are subjected to RA 10173 or the Data Privacy Act of 2012012 and RA10175 or the Cybercrime Prevention Act of 2012), stigmatization and discrimination on patients and loss of trust and reputation. To enable GHS fully to utilize the benefits of digitalization, the sector must institutionalize cybersecurity services in its functional description resulting in the prioritization and implementation of security-related programs, manuals, and frameworks.

2. **Implementing proactive response and detection to cybersecurity incidents that will provide continuous and centralized visibility of GHS digital architecture thus resulting in effective and efficient cybersecurity incident management.** – As cybersecurity attacks become more progressive and complex, anticipating future needs, problems, and changes must be addressed appropriately thus preventing successful attacks from taking place. Identification and detection of an incident and event are critical activities in cybersecurity management. Proper, effective, and responsive monitoring and analysis is one of the key aspects of proactive cybersecurity by knowing all the digital activities that are happening under its control. According to the Mandiant Security Effectiveness Report of 2020, 58% of the hackers penetrated an enterprise infrastructure unnoticed while 91% of attacks did not generate an alert. Additionally, according to IBM and Blumira's report on 2021, the average lifecycle takes 287 days, with 212 days to initially detect and 75 days to mitigate. Moreover, proactive cybersecurity includes controls that will maintain and analyze the logs to provide quick and responsive identification in the occurrence of malicious cybersecurity events. This also covers vulnerability assessment to identify threats prior to and post-deployment activities.

   Improved Cybersecurity Architecture – The utilization of higher model of cybersecurity components will improve the performance of NCMH Cybersecurity Posture. This will result in easier management, availability, and better performance. Additionally, in the Philippine Government Health Sector setting, according to the National Cybersecurity Plan of 2022, the health sector is considered one of the critical infostructure (CII) of our government. In line with this, to establish the resiliency of the CIIs, the government has launched strategies and programs to achieve a "Resilient Enterprise State" that has the objective to have predictive and mission-focused to continue operations through cyber-attacks (NCSP 2022). Moreover, according to DICT department circular no. 003, all bureaus, offices, agencies, and instrumentalities of the Philippine Government that handle critical ICT infrastructure are mandated to establish their own Computer Emergency Response Team (CERT) as a proactive mechanism in the detection, response, and mitigation of cyberattacks and digital threats and vulnerabilities.

3. **Secured Digital Environment** – The most effective cybersecurity programs combine two security concepts: defense-in-depth and threat-based modeling (Broughton, K., 2017). In the practice of the defense-in-depth model, cybersecurity design, and management must be implemented in layers and levels of protection for network and systems security. Different electronic systems and network security tools such as Intrusion Prevention/Detection Systems (IPS/IDS), firewalls, and other network security devices are designed to be integrated into a single network infrastructure and are implemented throughout the security architecture. Moreover, to ensure the effectiveness of this strategy, different security controls such as physical security, and organizational controls including policies, guidelines, and frameworks must be included in the design and implemented accordingly to aid the latter security control. Additionally, these different controls must be working in synchronization to make the defense-in-depth model effective (Groat, S., Tront, J., et.al., 2013). n the other hand, threat-based models focus cybersecurity implementation on the classification and criticality of ICT resources. The more critical the resource is, the more defenses will be implemented adjacent to it (Broughton, K., 2017). This model also indicates that, generally, every organization had no unlimited resources to deploy every technology and strategy in its architecture so, to compensate for that lack, ideally, organizations resorted to risk-based approaches wherein it prioritizes the most probable threat and vulnerability that can be exploited.

III. SCOPE OF WORKS

A. General Works

1. Delivery, configure, deploy, and commission the procured NCMH Endpoint Security License
2. The bidder must configure the procured Endpoint Security License based on the configuration provided by NCMH IHOMP/IT Unit
3. During the deployment and configuration, the supplier must ensure that the activity will only have minimal to no business disruptions.
4. The bidder must provide all components, cables, modules, or devices that are necessary for the project. The bidder must consult the system administrator for their preferred schedule before doing any major installation and/or fixes.
5. Define and configure administrative and system security policies, practices, and codes.
6. Prepare a hardened system and turnover of administrative rights to NCMH.
7. Test and debug the deployed NCMH Endpoint Security.
8. The bidder must provide detailed technical documentation of the project.
9. Any improvement and/or supplemental to the conceptual design, quantity, and/or deemed necessary to attain functionality, integrity, security, and completion of the project must be shouldered by the bidder with no additional cost.
10. Other works and materials that may have been omitted here but are necessary to put the system in operation and to complete the works to commission and implement the system within the required period.
11. Bidder must provide manufacturer-certified next-generation firewall professional full course training on the existing network engineering technology.
    i. Curriculum-based and manufacturer training from a certified training center for two (2) NCMH network administrators on the following but not limited to installing, configuring, administration, and management of the endpoint security platform.

B. Technical Specifications

The specifications for the renewal of NCMH endpoint security will be the following:

1. NCMH Endpoint Security for Workstations

   a. Must be cloud-based
   b. Web Security
   c. Download Reputation

d. Web Control / Category-based URL Blocking
e. Peripheral Control
f. Application Control
g. Deep Learning Malware Detection
h. Anti-Malware File Scanning
i. Live Protection
j. Pre-execution Behavior Analysis (HIPS)
k. Intrusion Prevention System
l. Potentially Unwanted Application (PUA) Blocking
m. Data Loss Prevention
n. Runtime Behavior Analysis (HIPS)
o. Antimalware Scan Interface (AMSI)
p. Malicious Traffic Detection (MTD)
q. Exploit Prevention
r. Active Adversary Mitigations
s. Ransomware File Protection (CryptoGuard)
t. Disk and Boot Record Protection (WipeGuard)
u. Man-in-the-Browser Protection (Safe Browsing)
v. Enhanced Application Lockdown
w. Threat Cases (Root Cause Analysis)
x. Automated Malware Removal
y. Synchronized Security Heartbeat
z. Integrated ZTNA agent
aa. Must be integrated to existing NCMH NGFW

2. **NCMH Endpoint Security for Servers**

a. Must be Cloud based
b. Web Security
c. Download Reputation
d. Web Control / Category-based URL Blocking
e. Peripheral Control
f. Application Control
g. Application Whitelisting (Server Lockdown)

h. Deep Learning Malware Detection
i. Anti-Malware File Scanning
j. Live Protection
k. Pre-execution Behavior Analysis (HIPS)
l. Potentially Unwanted Application (PUA) Blocking
m. Intrusion Prevention System
n. Data Loss Prevention
o. Runtime Behavior Analysis (HIPS)
p. Antimalware Scan Interface (AMSI)
q. Malicious Traffic Detection (MTD)
r. Exploit Prevention
s. Active Adversary Mitigations
t. Ransomware File Protection (CryptoGuard)
u. Disk and Boot Record Protection (WipeGuard)
v. Man-in-the-Browser Protection (Safe Browsing)
w. Enhanced Application Lockdown
x. Threat Cases (Root Cause Analysis)
y. Automated Malware Removal
z. Synchronized Security Heartbeat
aa. Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform)
bb. Synchronized Application Control (visibility of applications)
cc. Cloud Security Posture Management (monitor AWS, Azure, GCP environments)
dd. Server-specific Policy Management
ee. Update Cache and Message Relay
ff. Automatic Scanning Exclusions
gg. File Integrity Monitoring
hh. Must be integrated to existing NCMH NGFW

IV. EXPECTED DELIVERABLES

1. 200 renewed, configured, and installed NCMH Endpoint Security Licenses

2. 200 additional, configured and installed NCMH Endpoint Security Licenses
3. 4 renewed, configured, and installed NCMH Endpoint Security for Servers Licenses
4. 6 additional, configured, and installed NCMH Endpoint Security Licenses for Linux Server
5. 4 additional, configured and installed NCMH Endpoint Security Licenses for Windows Server

V. IMPLEMENTATION ARRANGEMENTS INCLUDING ROLES AND RESPONSIBILITIES

Within the Project duration the NCMH shall:

1. Provide a technical working committee to supervise and monitor the project.
2. Provide a technical contact person
3. Facilitate access to information, documents, facilities and other necessary things needed by the contractor to perform services.
4. Assist in coordinating with and issue instructions as may be necessary or appropriate to other government agencies for the prompt and effective implementation of the services.
5. Approve the proposed working schedule of the supplier.
6. Provide temporary ID to all personnel involved in the installation
7. Grant authorized representative access to premises as well as equipment and all facilities located therein to perform the supplier's obligations.
8. Make prompt review and revision, if necessary, which shall be not later than ten (10) working days from receipt of the work produced.
9. Pay the contractor upon presentation of requisite documents, the amount due him upon receipt of claims supported with documents subject to acceptance by the NCMH.

Within the Project duration the winning Contractor/Supplier shall:

1. Perform services professionally based on industry standards and always protect the interest of the government in general and NCMH.
2. Provide list of certified engineers/technical support team with addresses and contact numbers, involved and other activities related to the project.
3. Secure for the NCMH permits, licenses, and approvals that are or may be necessary to perform services.

4. Provide a chief officer or program manager (licensed ECE, COE or EE) who will be directly in charge of managing the project, and day-to-day contact personnel in charge of operations.
5. Complete the delivery, installation, and configuration within sixty (60) calendar days from the receipt of the Notice to Proceed. Otherwise, the winning Service Provider/Bidder shall pay the corresponding penalties/liquidated damages in the amount of one-tenth of one percent (1/10 of 1%) of the total contract price for every calendar day of delay.
6. Submit a proposed working schedule for approval of NCMH and secure a security pass and working permit on their site.
7. Ensure that all personnel involved in the project are in proper uniform because it will be their identification from the rest of NCMH's employees and visitors.
8. Protect the privacy of NCMH and ensure that all confidential information and data on its ICT infrastructure are kept confidential.

VII. QUALIFICATION OF THE SUPPLIER

1. Bidder must attach to his/her proposal an assurance from his/her principal that the items called for will be supplied in full and on time
2. Extensive knowledge, background and technical experience in a great number of projects covering Endpoint Security.
3. Should have been engaged for at least five (5) years in various ICT services such as IT project management, computer networking and security, voice and data communications infrastructure development, and ICT facilities operation and management.
4. The bidder should have locally-based Manufacturer Certified Engineers who will do the installation, configuration, and after-sales support of all proposed equipment for endpoint security
5. Must have a 24x7 helpdesk support system.
6. All proposed items must be certified genuine and brand new. Bidder must be an authorized Philippine Distributor, Dealer or Value-Added Reseller of his/her proposed products and must provide local technical services on these.

VIII. ADDITIONAL REQUIREMENTS TO BE SUBMITTED WITH TECHNICAL PROPOSAL

1. Plan of Approach and Methodology
2. Complete technology solution offered including detailed specifications.
3. Corporate Profile which should include major achievements, service Portfolio or services offered by the firm, experience or engagements both local and international.
4. List of engineers.
5. Draft of Service Level Agreement

IX. WARRANTY PERIOD AND SERVICES

1. Period: Three (3) years of support services are required on all delivered goods and shall take effect immediately after final acceptance of the project with NCMH.
2. Product upgrades:
   i. Provision, supply, and installation of announced improvements on the proposed product and/or any of its components, after the date of submission of proposals and before the date of implementation in the project sites without additional costs to NCMH.
   ii. Provision or entitlement of all applicable upgrades including firmware or software upgrades without additional cost to NCMH.

Prepared by:

Engr. William Wallace L. Arias, ECE
OIC, IHOMP/IT Unit
National Center for Mental Health

Approved by:

Dr. Noel V. Reyes, MD, FPPA, MMHoA
Medical Center Chief II
National Center for Mental Health