HELLENIC ELECTRICITY DISTRIBUTION NETWORK OPERATOR S.A.

NOTICE OF CALL FOR TENDERS No ND-207

PROJECT: "Pilot Telemetering and Management System for the Electric Power Supply Demand by Residential and Small Commercial Consumers and Implementation of Smart Grids"

MINIMUM SECURITY REQUIREMENTS FOR THE PROJECT

CONTENTS

1 Overview

All the systems and the operations of the project must be secure from any unauthorized access, intentional or unintentional, must be constantly monitored and updated to ensure that any threats are detected and eliminated before they have any type of impact on the system, the utility or the consumer.

As automated control of energy assets migrates with gradual modern technology applications like "smart grids", security and access control to infrastructures, both from within the utility as from outside has become critical.

Physical and logical security must be implemented at all levels in order to ensure the safe and efficient operation of the monitoring and control subsystems. Physical security – controlling access to the control room for example, combined with logical security – using information systems to restrict access to monitoring and control functions – provides an initial framework upon which to specify and operate a security infrastructure that ensures business objectives are attained while minimizing risk.

Utility systems of the future will be a patchwork of subsystems – as new capabilities are added to the utility infrastructure, existing systems must operate together with these newer systems in a manner that does not increase vulnerabilities at the interconnections, or does not introduce security risks in the co-operation of applications/subsystems.

Managing security risks requires that all business processes be firmly established and documented. In the case of the AMI/MDM system, all processes surrounding the collection of data, whether installation or data that is received from the consumer, must be understood and documented prior to the installation of the AMI/MDM system.

As the AMI/MDM systems are deployed and operated, all vulnerabilities and threats must be identified and addressed constantly, in a clearly documented manner. To this end, comprehensive security plans must be developed and implemented such that threats are under control and results are as expected with the mitigate strategies in place.

2 Physical Security Requirements

1. The Contractor shall document use cases associated with the collection and management of customer data with respect to physical security practices and present risks/vulnerabilities analysis. Based on this analysis, the contractor shall determine the process amendements for the the AMI/MDM system implementation and shall identify where risks are reduced, maintained, or increased.
2. Contractor shall document use cases associated with physical security to all attended and unattended facilities associated with the AMI/MDM system. Those facilities include control centers, communication facilities, data storage

areas, back up areas, etc.

3. Contractor shall establish and operate a physical security perimeter to all attended and unattended facilities associated with the AMI/MDM system. This is to include control centers, communication facilities, data storage areas, back up areas, etc.
4. Contractor shall establish and ensure that all personnel with physical access to critical facilities have authorized access only to the level necessary to perform their required duties.
5. Contractor shall supply and install all necessary equipment, establish and operate a process that describes entry-to-exit monitoring of physical access for individuals, including but not limited to:
   - Video monitoring of control centers, communication facilities, data storage areas, back up areas, and main access areas.
   - Recording with access control system for all individuals entering and departing critical infrastructure assets, including control centers, communication facilities, data storage areas, back up areas, and key passageways that personnel is using.
6. Contractor shall develop and implement a site response plan for each critical infrastructure for which the Contractor is responsible. The primary goal of the site response plan is to differentiate normal electrical or mechanical failures from malicious acts. For events that are normal electrical or mechanical failures, a process shall be in place to notify HEDNO of the need for corrective action. For events that are determined to be malicious, a process shall be in place to notify security personnel as well as HEDNO and a process shall be in place to further restrict access to the affected area.
7. Contractor shall ensure that personnel associated with critical site access privileges is suitable and appropriate for unescorted site access.
8. Contractor shall ensure that all contractor and subcontractors personnel are aware of HEDNO security practices and fully follws them. All contractor personnel shall sign acknowledgements that they understand and will act according to HEDNO confidentiality and security measures.
9. Contractor shall ensure that physical and logical access to all systems is validated using a proper system (e.g key-card). Contractor shall ensure that key-card must remain inserted at a specific workstation for the log-on to persist, e.g. once logged on to the system, removal of the card will force an automatic log-out.

3 Logical Security Requirements

10. Contractor shall document use cases established at HEDNO associated with the collection and management of customer data with respect to logical security practices and present risks/vulnerabilities. Contractor shall

determine the changes to these established use cases by implementation of the AMI/MDM system and Contractor shall identify where risks are reduced, maintained, or increased as a result of the new AMI/MDM implementation.

11. Contractor shall develop, document and operate a process for authentication of users at all levels within the AMI/MDM system. Contractor shall ensure that the process uses secure authentication methods for the revocation or assignment of user permissions as required.

12. Contractor shall ensure and demonstrate that authentication processes support emergency operations and that such authentication processes are not an impediment to operations at critical times.

13. Contractor shall ensure that all passwords are uniquely generated by a corresponding service or that the system coerces the user to change the password upon entry to the system.

14. Contractor shall ensure that all user accounts have "strong" passwords and that the user will be coerced to develop such passwords if not provided to the user.

15. Contractor shall ensure that all root-access roles utilize an internally-generated security key and that root access is not permitted for accounts where user-specified passwords are enabled.

16. Contractor shall ensure that all user accounts conform to a role-based hierarchy such that permissions are granted based upon the role of the user.

17. Contractor shall ensure that when a user is removed from the central system or otherwise is not associated with the project that the user's access to all systems is terminated.

18. Contractor shall ensure that end-to-end encryption is used for all network information traffic, including meter to MDM or consumer/mobile application to mobile platform.

19. Contractor shall document implementations of encryption within the AMI/MDM system.

20. Contractor shall certify that a minimum encryption of AES 128bit has been implemented for meter to MDM communications.

21. Contractor shall provide documentation regarding the end-to-end security methodology, including meter to in-home device and AMI/MDM to consumer.

22. Contractor shall ensure that unnecessary services and programs bundled with the vendor's software but not in use at HEDNO (for whatever reason) is disabled or removed so as not to present a security vulnerability. Contractor shall document such implementations.

4 Protection of Consumer Data

23. Contractor shall certify and demonstrate compliance with the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Meterings Systems[1].

5 Documentation of Security Requirements

24. The Contractor shall submit a Security Architecture Study for the system. The goal of this study shall be to document all technical and operational requirements and, according to the study to design a suitable security architecture both at the network and systems level and at the Web application level. The study shall ensure that all significant security parameters have been included in the implementation specifications of the overall IT system (Security by Design).
25. The Contractor is required to develop and implement Secure Configuration Guides. Thus it shall be possible for the system to be configured according to certain rules and optimum security practices. The goal is to develop technical guidelines for secure configuration of all modules constituting the System and to implement thereof in the system prior to its integration in the production. In particular, safe configuration guidelines shall be developed and implemented at minimum for the following:
    - The databases
    - The Internet servers (e.g. IIS X.X Secure Configuration guide, Apache X.X Secure Configuration guide etc.)
    - The operating systems where the databases shall be hosted, and the
    - Internet servers.
    - The Firewalls

26. Prior to the integration of the system in the production, it is required to perform Penetration Tests, both at the system and network level (System & Network Penetration Test) and at the Web application level (Web Application Penetration Test). The profiles emulated by the Penetration Tests shall be at minimum:

    - System & Network Penetration Test:
        a) External user without access rights
        b) Internal user without access rights
        c) Internal user with access rights

    - Web Application Penetration Test
        a) User with access rights
        b) User without access rights

[1] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

27. Contractor shall design and conduct penetration testing, in cooperation with a third party penetration tester, for an assesment of the overall security of the system to be delivered. HEDNO will approve this design. The contractor will recommend three independent certified institutions to perform the penetration testing and HEDNO will choose one of those to conduct the final test. The contractor is obliged to take all necessary action to correct any problems that may arise during the execution of the tests. The success of the test results will be certified by the third party institution.
28. The Contractor shall submit a system security manual describing in detail the procedures that should be followed to ensure that system security is not in any case reduced.
29. The above-mentioned penetration tests procedure will be repeated on a per annum basis.
30. The cost for these tests for the five – year operation of the system, must be included in Contractor's offer.

6 HEDNO's Information Systems Security Framework

31. Besides what is presented in this issue, the offered system shall meet the HEDNO's Security Framework for Information Systems, according to the attached to this issue Annex:
    - HEDNO's Standard for Access Codes (passwords) (ΠΑ-1)
    - Security Standard for IT Applications of HEDNO (ΠΑ-2)
    - Operation Standard for IT Systems of HEDNO (ΠΑ-3)

7 ANNEX

The Annex is available only in Greek language and includes the following HEDNO standards:

- HEDNO's Standard for Access Codes (passwords) (ΠΑ-1)
- Security Standard for IT Applications of HEDNO (ΠΑ-2)
- Operation Standard for IT Systems of HEDNO (ΠΑ-3)