

**APPROVE ENTERING INTO AN AGREEMENT WITH DIAMOND MANAGEMENT &
TECHNOLOGY CONSULTANTS NA, INC. FOR IMPLEMENTATION OF INFORMATION SECURITY
SERVICES PROGRAM**

THE CHIEF EXECUTIVE OFFICER REPORTS THE FOLLOWING DECISION:

Approve entering into an agreement with Diamond Management & Technology Consultants NA, Inc. ("Diamond") to implement an information security services program for Information & Technology Services at a cost not to exceed \$950,000.00. Vendor was selected on a competitive basis pursuant to Board Rule 5-4.1.

A written agreement for Vendor's services is currently being negotiated. No services shall be provided by Vendor and no payment shall be made to Vendor prior to the execution of the written agreement. The authority granted herein shall automatically rescind in the event a written agreement is not executed within 90 days of the date of this Board Report. Information pertinent to this agreement is stated below.

SPECIFICATION #: 07-250040

VENDOR: Diamond Management & Technology Consultants NA, Inc.
875 N. Michigan Ave., Suite 3000
Chicago, IL 60611
Contact Person: Chris O'Brien
Phone: (312) 255- 5770
Vendor # 85053

USER: Information & Technology Services
125 S. Clark, 3rd Floor
Chicago, IL 60603
Contact Person: Robert Runcie
Phone: (773) 553-1300

TERM: The term of this agreement shall commence on the date the agreement is signed and shall end one (1) year from contract commencement. This agreement shall have one (1) option to renew for a period of one (1) year.

SCOPE OF SERVICES: The Vendor will provide services for two main projects, an Information Security Management System (ISMS) and an Information Security Risk Assessment. The description of these services is as follows:

I. Information Security Management System (ISMS)

- a. The Vendor will provide an Enterprise Information Security Management System (ISMS) to operate as a management body for the development and execution of an ISO 27001 style security program. The ISO 17799:2005/27001 code of practice for information security management includes recommendations for 133 different controls in 11 categories aimed at reducing risks to the confidentiality, integrity and availability of the subject information.
- b. The ISMS shall meet the following goals:
 - i. The ISMS shall identify information security goals that meet the Board's requirements and develop staffing profiles to ensure there are adequate resources to achieve them.
 - ii. The ISMS shall catalog and review the Board's information security related policies and develop a policy framework to ensure that information security objectives and plans are established, and address how roles and responsibilities should be allocated within the organization with respect to the policy.
 - iii. The ISMS shall catalog key organizational information assets, assess program level threats, and develop a process for deciding (within the context of any existing organizational risk treatment framework) acceptable levels of risk and ensuring that awareness of these threats is communicated to applicable audiences.
 - iv. The ISMS shall direct the development of an information security awareness program.

- v. The ISMS shall direct the development of an incident response process capable of promptly detecting and responding to incidents, as well as the review and oversight of information security incidents, and receiving reports from the information security manager on the status and progress of specific implementations, security threats, results of reviews, audits, etc. and ensuring adequate steps are taken to implement any findings.
- vi. The ISMS shall develop an approval process for major initiatives (such as any individual initiative associated with the implementation of ISO/IEC 27001) to improve information security within the organization.
- vii. The ISMS shall establish a means of ensuring and measuring compliance with policy and reviewing these metrics periodically.

II. Information Security Risk Assessment

- a. The Vendor will conduct in person interviews with business and technical staff, identify assets/data, and review existing architecture, processes, policies, etc. in order to document and catalog the existing CPS environment and properly assess requirements. Based on results of the risk assessment, the Vendor will develop a compendium of recommendations for the deployment of mitigation actions or strategies for Chicago Public Schools, intended to limit losses and determine appropriate safeguards.
- b. The Vendor will catalog and evaluate physical and logical assets. The evaluation will be done using a risk assessment methodology.
- c. Vendor will provide a list of the business areas, staff positions, and subject matter experts the respondent expects to interview to conduct the asset discovery.

DELIVERABLES: Vendor will provide the following deliverables with respect to each project:

I. ISMS

- a. Help size and scope an effective ISMS for CPS
- b. Define roles of ISMS members
- c. Review of the current CPS org chart to determine membership
- d. Assist in the creation of an ISMS charter to be instituted as policy by the Board of Education
- e. Develop the tactical and strategic process catalog for the ISMS
- f. Provide training sessions and materials for existing ISMS members
- g. Develop training materials for each ISMS role so that future members have sufficient material to successfully participate in ISMS processes.
- h. Guide and provide expertise to the ISMS in the formation of the Statement of Applicability (SOA) for the security program.
- i. Provide recommendations for a security and risk management team and how it will function in the future.
- j. Facilitate initial meetings to guide the ISMS through initial projects - SOA development and Information Security Risk assessment.

II. Information Risk Assessment

- a. Vendor will provide a report listing categories of information assets (physical and logical) used by CPS
- b. Vendor will provide a reports which should, at minimum address the following concerns:
 - i. Identify threats and likelihood of those threats materializing
 - ii. Identify and rank critical assets and operations
 - iii. Identify potential vulnerabilities in critical assets and operations
 - iv. Estimate potential damage due to identified threat or exploitation of vulnerability
 - v. Identify cost effective mitigating controls and provide cost/benefit analysis

OUTCOMES: Vendor's services will result in a program plan for an ISO 27001 Information Security Management System that will guide the development of the Board's security program and provide an enterprise information security risk assessment for the organization to provide an initial foundation of assessment data to guide the Board's ISMS in prioritizing activities.

COMPENSATION: Consultant shall be paid as specified in the agreement; total compensation shall not exceed \$950,000.

REIMBURSABLE EXPENSES: None.

AUTHORIZATION: Authorize the General Counsel to include other relevant terms and conditions in the written agreement. Authorize the President and Secretary to execute the agreement. Authorize Chief Information Officer to execute all ancillary documents required to administer or effectuate this agreement.

AFFIRMATIVE ACTION: This contract is in full compliance with the goals required by the Revised Remedial Plan for Minority and Women Business Enterprise Contract Participation (M/WBE Plan). The M/WBE participation goals for this contract include 25% total MBE and 5% total WBE.

Diamond Management & Technology Consultants NA, Inc has identified the following firms and percentages:

Total 30% MBE:

Senryo Technologies, Inc 30%
1300 Iroquois Avenue, Suite 155
Naperville, IL 60563

Total WBE 7%:

Monarch Group, Inc. 7%
150 N. Wacker Drive #2140
Chicago, IL 60606

LSC REVIEW: Local School Council approval is not applicable to this report.

FINANCIAL: Charge to Information & Technology Services: \$950,000.00 FY08
Budget Classification: 12510-115-54125-009580-000000-2008 \$400,000.00
12510-115-54125-009580-000000-2009 \$450,000.00

GENERAL CONDITIONS:

Inspector General – Each party to the agreement shall acknowledge that, in accordance with 105 ILCS 5/34-13.1, the Inspector General of the Chicago Board of Education has the authority to conduct certain investigations and that the Inspector General shall have access to all information and personnel necessary to conduct those investigations.

Conflicts – The agreement shall not be legally binding on the Board if entered into in violation of the provisions of 105 ILCS 5/34-21.3 which restricts the employment of, or the letting of contracts to, former Board members during the one year period following expiration or other termination of their terms of office.

Indebtedness – The Board's Indebtedness Policy adopted June 26, 1996 (96-0626-PO3), as amended from time to time, shall be incorporated into and made a part of the agreement.

Ethics – The Board's Ethics Code adopted June 23, 2004 (04-0623-PO4), as amended from time to time, shall be incorporated into and made a part of the agreement.

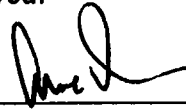
Contingent Liability – The agreement shall contain the clause that any expenditure beyond the current fiscal year is deemed a contingent liability, subject to appropriation in the subsequent fiscal year budget(s).

Approved for Consideration:



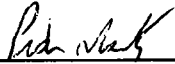
Heather A. Obora
Chief Purchasing Officer

Approved:



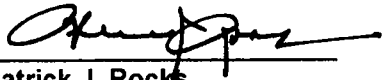
Arne Duncan
Chief Executive Officer

Within Appropriation:



Pedro Martinez
Chief Financial Officer

Approved as to legal form



Patrick J. Rocks
General Counsel