REPORT NO: 09-12
DATE: March 17, 2009
ANALYST: Betty J. Stanifer

CLASSIFICATION REPORT

PROPOSED TITLE:	Deputy Director, BIS Information Security (Appointed)
CURRENT TITLE:	New Position
INCUMBENT:	Vacant
REASON FOR REQUEST:	Evaluation to ensure proper classification of a proposed Appointed Position for Information Security
DATE QUESTIONNAIRE SUBMITTED:	3-11-09
DATE OF PREVIOUS STUDY:	---
DISPOSITION OF PREVIOUS STUDY:	---
PERSONS INTERVIEWED:	Lynn Willenbring; Chief Information Officer
RECOMMENDATION:	Establish the Deputy Director, BIS Information Security (Appointed) allocated to Grade 13 with 590 Total Points using vacant position no. 259 as a funding source.

The Business Information Systems Department is proposing that an Appointed Information Security Officer position be established that will report to the Chief Information Officer directly. Currently there is no position responsible for directing the information security program of the city of Minneapolis; the position will assess risk, recommend risk mitigation strategies, oversee implementation and ensure compliance to ensure data security for the entire enterprise. The incumbent will work with the contracted service provider to ensure data security, including protection from

network breech, application security, etc. In the event that the position believes that significant risk remains in the environment the incumbent will inform the Chief Information Officer for final risk management strategy determination. The request for evaluation has been submitted to the Classifications Unit to ensure the appropriate placement of the position in the hierarchy. The position will be responsible for but not limited to the performance of the following duties.

- Architect, implement and monitor an enterprise wide information security program, ensuring the security integrity, privacy and availability of information and systems.
- Advocate and protect enterprise security by serving as a key information security advisor for executive staff and the organization.
- Develop, deploy and champion enterprise wide training programs in information security awareness.
- Assess the City's information risks; develop, public, and maintain appropriate policies, processes, and standards to protect the City.
- Work closely with the outsourcing service provider's information security personnel to ensure risks are addressed and mitigated in a timely, cost effective, and appropriate manner.
- Ensure the security of the remote and mobile computing environment.
- Guide management on information security matters, such as department-specific policy, state and federal laws, industry related regulations, the City's privacy policies and industry best practices, and determine the effect on initiatives, projects, and business operations.
- Act as the City's official information security representative to internal customers, external partners, and audit and regulatory.
- Coordinate highly confidential information security breach and computer-fraud related investigations facilitating legal, human resources, management, and law enforcement involvement as needed.
- Work closely with internal and outsourced technology infrastructure and application groups to research, evaluate, design, implement and maintain all new and improved information technologies for the enterprise.
- Evaluate and provide direction in matters of information security privacy and privacy protection best practices.
- Proactively test and protect the integrity, confidentiality, and availability of information within the enterprise within the context of the security policies.
- Evaluate suspected security breaches and recommend corrective actions.
- Manage security related service level agreements with outsourcing service provider and other outside suppliers of information protection services or data hosting. Recommend modifications and negotiate changes as directed.
- Develop and maintain effective business continuity and disaster recovery plans, processes and procedures necessary to recover business services in the event of a declared disaster. Provide consultative services to business units in the development of these plans. Maintain and communicate an enterprise wide scorecard of disaster recovery readiness and serve as the City's focal point for information security incident response planning, execution and awareness.
- Develop appropriate criteria needed to assess the compliance of security standards by new and existing personnel, applications, IT infrastructure, and physical facilities.
- Develop information security training for new hires and existing staff, ensuring security awareness and adherence to best practices.

POSITION ANALYSIS

PRE-REQUISITE KNOWLEDGE

Candidates applying for the position are required to have a Bachelors Degree in Computer Science (Masters Degree preferable), a relate field or equivalent and five years of technology industry experience that demonstrates a high level of expertise in information security and a wide exposure to all aspects of information technology. This would include broad experience with information-security focused technologies, such as intrusion detection, firewalls, Public Key Infrastructure (PKI), Virtual Private Network (VPN), remote computing, authentication, biometrics, smart cards, etc. Additionally, the department position requires that candidates be certified as the following: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), or Certified Information Systems Management (CISM) would be acceptable.

The individual hired would need broad knowledge of information–security focused technologies; knowledge of distributed information technology architecture; and general knowledge of all aspects of information technology. The incumbent would need proven ability to communicate complex information security concepts and develop business case justifications to influence multiple levels of decision-makers; ability to manage key vendor relationships for delivering outsourced security solutions; ability to relate business requirements and risks to technology implementation for security related issues; and the ability to work well in stressful situations. Confidence and leadership skills are necessary to manage cross functional teams on simultaneous projects; as well strong consensus building and influence management skills, strong verbal and written communication skills, and strong project management and leadership skills.

The proposed position would not require the breadth of knowledge or experience that is required of the Chief Information Officer (Appointed) or the Director, Business Information Systems (Appointed) positions. It would be more in line with the pre-requisites attached to the Deputy Director, Managed Services BIS (Appointed) and the Manager, Business Information Services (Appointed). A rating of 70 is being applied.

DECISIONS AND ACTIONS

The position will have considerable latitude in making decisions and taking action on information security being the department expert in this area. Decisions to shut down network or server access, effectively idling thousands of City staff to isolate a threat is made in the moment, based on an understanding of the technology environment, impact upon City operations, consequence of error, and nature of the threat. Problems encountered most frequently including determining the urgency of applying security patches, evaluating threat vulnerabilities and implementing immediate mitigation strategies.

Any proposed policy changes and operational decisions which would have a significant financial cost or significant impact on the City's ability to perform functions would be reviewed and approved by the Chief Information Officer.

Security industry best practices; federal, state and local laws; and experience are frequently used resources in making decisions, resolving problems or taking other actions.

The impact of decisions and actions made by the proposed position would be greater than those of the Manager, Business Information Services (Appointed) who's areas of decision making focuses on specific areas within the department and would have an internal impact. An error in decisions or actions taken by the position under evaluation would have a damaging affect on the reputation of the City and lost of data could potentially effect City residents/customers that the City provides various services for; i.e., loss of personal information that could result in identity theft. On this factor the position is comparable to the Directors, BIS (Appointed) and other executive level position that are allowed considerable latitude in directing the quality assurance methodologies of complex IT solutions, along with the planning, development, coordination, and installation of applications and technology to address the information needs of the City and its customers. A rating of 70 is warranted on this factor.

SUPERVISORY RESPONSIBILITY

As the position is currently proposed to be structured; the incumbent will have no supervisory responsibility and is being allotted no credit on this factor.

RELATIONSHIPS RESPONSIBILITY

Contacts experienced by the proposed position will be on a weekly to semi-annual basis and although less frequent than those experienced by other executive level positions in the department they are of equal importance. Internal contacts with be with the CIO for direction and to advise on security issues weekly; with BIS Directors to advise on security issues weekly; with BIS Managers to review security and direct changes weekly; with other City Department Liaisons to explain and implement security practice and changes monthly; with City staff to oversee and/or conduct training quarterly; with Department Heads to recommend security practice changes monthly; and with City Council to present policy changes for approval semi-annually.

External contacts are with service providers to oversee security practices, develop standards and ensure implementation weekly and with the State Information Security Council monthly to represent the City's interest in State decisions and provide input into the decisions made by the State Information Security Council.

These contacts appear to be parallel to those experienced by the Director's BIS (Appointed), but the incumbent's ability to deal with people is not as crucial to the success of the position as that of the Director, BIS. The position under evaluation works more in the background to ensure information security. A rating comparable to what is assigned the appointed positions Deputy Director, Managed Services and Manager, Business Information Services would be in order. A rating of 60 is being applied.

WORKING CONDITIONS

The working conditions are comparable to other executive level and managerial positions in the department that work in an office setting with daily exposure to computers. Based on this comparison, a rating of 20 is being applied.

EFFORT

The position will be under significant pressure when facing information security threats that could impact all City operations shutting down network or server access, and idling City staff, which causes the incumbent considerable mental stress. Assessing risk, recommending risk mitigation strategies, ensuring compliance, and developing security policies and training is a major part of the job. The incumbent works with Unisys on the physical side of data security; network breech, system breech, application security, (i.e., Utility Billing) etc. It is also being taken into consideration that the position serves as the City's focal point for information security incident response planning, execution and awareness placing more stress on this position. There is justification to assign a rating of 70 on this factor taking into consideration the nature of the work and the pressures involved.

CONCLUSION

The Chief Information Officer is the Appointing Authority for the proposed position and according the information provided the position meets the Criteria for Appointed Positions under the Minneapolis Code of Ordinance: Section 20.1010 as described below.

1. **The person occupying the position must repot to the Head of the designated City Department or the designated City Department Head's Deputy.**

   The Deputy Director, BIS Information Security will report directly to the Chief Information Officer.

2. **The person occupying the position must be a part of the designated Department Head's Management Team.**

   The position is part of the Chief Information Officer's Management Team.

3. **The duties of the position must involve significant discretion and substantial involvement in the development, interpretation or implementation of City or Department policy.**

   The Deputy Director, BIS Information Security (Appointed) will be responsible for development and implementation of information security standards for all City departments. S/he will recommend formal City policy for Council approval.

4. **The duties of the position must not primarily require technical expertise where continuity in the position would be significant.**

   The position duties will require industry-standard technical expertise that is reasonably available in the market place.

5. **There is a need for the person occupying the position to accountable to, loyal to, and compatible with the Mayor, City Council and the Department Head.**

   This is expected. In this position, in order to successfully execute responsibilities, the individual will be exercising great discretion and decision authority that must be done in cooperation with the goals and strategies of City Leaders.

RECOMMENDATION

Establish the Deputy Director, BIS Information Security (Appointed) allocated to Grade 13 with 590 Total Points using vacant position no. 259 as a funding source.