

Town of Wayland IT System and Security Status Update

July 10, 2015

Mike McCann, Advent Consulting, LLC *

This document provides an updated project status and assessment of the Town/School IT system in response to memo dated March 30, 2015 to Finance Committee from Nan Balmer, Town Administrator, RE: Information Technology: Current Year Transfer Request.

IT PROJECT TASKS:

- 1. IMPROVE SECURITY OF IT SYSTEM:** Review the recommendations of the contractor that is investigating recent cyber-attacks, examine existing IT security on joint IT systems and identify a program of immediate and ongoing actions and protocols. Supervise implementation of a new IT security program through IT staff.

Deliverable: IT Security System Description and Maintenance Protocol

Advent Consulting LLC was engaged to review recommendations of Elysium Digital and further assess security vulnerabilities and the IT systems to create a near-term prioritized plan of immediate and ongoing actions to improve the soundness of the IT systems and protocol and supervise its implementation through IT staff.

Project is in progress with expected completion by August 31, 2015.

Initial Status: Systems not maintained adequately to provide a high performance and secure computing environment. Major vulnerabilities identified:

- Microsoft Windows patching system was not providing patch status on the majority of computers in the Town government network.
- Antivirus software was missing from some systems.
- Application software was not being patched.
- Firewall logs were not being retained
- Unnecessary local administrator accounts existed on computers.
- Online banking authentication protocol provided by the Town's primary bank was weak.
- Major performance problems would periodically appear in the virtual desktop environment.

Accomplishments: An assessment of the IT systems was conducted to further identify security vulnerabilities. A short term tactical plan was developed to address the Elysium Digital recommendations and other identified IT issues discovered during the assessment. Oversight of IT staff was provided to implement all tasks of immediate need. A maintenance protocol was established for operating system and application patching. This is currently being handled on a partially automated basis that may not be sustainable long term.

Current Status: Systems have been brought to a satisfactory base level of security.

Recommended Next Steps: Remaining identified tasks that were determined to be of less-immediate need and requiring more time and resources are planned for the short-term tactical plan (Task 5).

Consider purchase of a product to automate maintenance tasks.

- 2. DEVELOP AND RECOMMEND IT SECURITY POLICY:** Review IT systems and develop an IT Security Policy appropriate for Wayland.

Deliverable: Wayland IT Security Policy

McGladrey LLP was engaged to provide IT Security Policies

Project is in progress with planned delivery by September 30, 2015.

- 3. TRAIN EMPLOYEES IN IT SECURITY TO PREVENT AND MITIGATE CYBER-ATTACKS:** Many cyber – attacks can be prevented through trained computer users, and the effects of a cyber – attack can be mitigated through planned response by employees. This task requires identifying and providing training appropriate for each job category, primarily town and school administrative employees.

Deliverable: Training and Materials

SANS Institute, in partnership with CIS Security, was engaged to provide user security training and materials for up to 1,200 users for one year (smallest purchase plan available).

Rollout of training is planned to begin in July 2015.

4. **TECHNICAL SUPPORT:** Provide technical support to IT staff under the direction of the Town Administrator and Superintendent primarily during the month of April when the IT Director will be chaperoning and teaching in the Wayland / Beijing Exchange Program. Technical support will be used as required in collaboration with existing IT personnel and will inform the plan in Task 5.

Deliverable: Log of IT Technical Support Requests and Response Provided

Advent Consulting LLC was engaged to provide technical support to IT staff both during the time when the IT Director was away and ongoing.

Project is in progress with expected completion by August 31, 2015.

Initial Status: IT staff required technical assistance and oversight to implement tasks identified in Task 1. A maintenance protocol to maintain a necessary level of system security was not in place.

Accomplishments: Technical support was provided to IT staff to implement tasks identified in Task 1 and Task 5 and will continue until project completion. Technical support was provided to IT staff to implement the established maintenance protocol for operating system and application patching and to inform to plan in Task 5.

Current Status: Working closely with IT staff systems continue to be maintained to a satisfactory base level of security.

Recommended Next Steps: Continued technical support and oversight of IT staff is necessary to continue to make progress toward implementation of identified system improvements.

5. **DEVELOP AND IMPLEMENT SHORT TERM TACTICAL PLAN:** Review existing IT systems and develop and supervise the implementation of short term plan of high impact / low cost tactical tasks and activities to improve the soundness of the IT system.

Deliverable: 3 Month Tactical Plan and Report of Actions Accomplished

Advent Consulting LLC was engaged to further review IT systems and develop and supervise the implementation of a short term plan of high impact/low cost tactical tasks to improve the soundness of the IT system and inform Town Administrator and School Superintendent in definition of scope of work to develop a long-range IT Capital Plan.

Project is in progress with expected completion by August 31, 2015.

Initial Status: Systems were brought to a satisfactory base level of security. However, tasks identified to bring systems to the next level of security remain are required to continue to improve the stability and security of the systems.

Accomplishments: A short term tactical plan of high impact/low cost tactical tasks and activities was developed to address these necessary tasks and oversight of IT staff was provided to implement these tasks.

Current Status: This Task is in progress with approximately 50% of these tasks complete.

Recommended Next Steps: Remaining security tasks are planned for completion by the end of August. The implementation of several additional system projects identified during the assessment are recommended.

6. **LONG RANGE IT CAPITAL PLAN AND JOINT IT MANAGEMENT, STAFFING & ORGANIZATION PLAN:** The conclusions from Tasks 1-5 above will inform the collaborative work of the Town Administrator and School Superintendent to define a scope of work to develop a long range IT Capital Plan and an IT Management, Staffing, and Organization Plan. The agreed upon plan will build on existing IT plans and will include but not be limited to: IT infrastructure including data storage and town and school administrative technology as well as IT security. The plans will require taking a look at the school / town IT organizational structure and the implications of any new structure for the IT annual operating budget and long term capital costs. Until this scope of work is established, the cost of the project is uncertain. A prior effort conducted by the Town in 2009 cost \$25,000.

Deliverable: Long Range IT Capital Plan and Joint Management, Staffing and Organization Plan

McGladrey LLP was engaged to provide an Information Technology Master Plan for the joint Town/School IT infrastructure, an IT Capital Plan and IT Management, Staffing, and Organization Plan. The agreed upon plan will build on existing IT plans and will include but not be limited to IT infrastructure including data storage and security and Town and School administrative technology. The

plan will require review of the Town/School IT organizational structure and the implications of any new structure for the IT annual operating budget and long-term capital costs.

Project is in progress with preliminary draft report planned for August, final report planned for September.

Recommendations to effectively manage the IT systems in the next fiscal year

To protect the Town against current and evolving IT security threats, improve manageability and system performance some capital expenditures will be required.

1. New firewall to improve perimeter security, logging and alerting to potential attacks.
Estimated cost \$30K.
Alternative is to continue with current firewall product.
2. Vulnerability and patch management software.
Estimated Cost: \$12K
Alternative is to continue to use semi-automated protocol in place today
3. Updated licenses for Servers.
Estimated Cost \$6K
Alternative is to consider outsourcing or retiring these servers where this is feasible, cost TBD.
4. Upgrade to backup software
Estimated Cost \$8K
Alternative is to continue using current software, though not efficient
5. Storage array replacement to improve performance increase storage space and reduce complexity.
Estimated Cost: \$70K
Alternative to continue with current storage is inefficient use of IT staff time to support and contributes to instability of systems.

Recommendation on staffing and management

The School Department supports a large number of end users with a continual increase in technology requirements, that require the IT Director's complete focus. Therefore, I recommend an IT organization to exclusively focus on the widely varying IT needs of the remaining Town Departments and the critical systems and security operations and maintenance of the joint Town/School infrastructure consisting of the following positions:

IT Director

- Reports jointly to Town Administrator and Superintendent of Schools
- Supervises Network/Infrastructure Admin and User Support Tech
- Responsible for IT strategy development and implantation for Town Departments

Network/Infrastructure Admin

- Reports to IT Director
- Maintains Virtual Infrastructure, Storage Systems, and Town Wide Network.

User Support Tech

- Reports to Town IT Director
- Provides application and desktop support to end users in Town Departments
- Handles phone system change requests and problem reports
- Monitors data backup

*** Note responses to Tasks 2, 3 and 6 provided by Elizabeth Doucette**