

COMMISSIONERS MEETING

Agenda

Wednesday, May 3, 2023

This meeting will be conducted in person
and electronically (via Zoom) at the

Cheshire County Department of Corrections
825 Marlboro Road, Keene, NH

Zoom Call-in Number: +1 646 558 8656

Meeting ID: 409 748 8803

Pin #: 6031233

Start Time 08:30 AM

Present: Commissioners Jack Wozmak, Robert Englund, and Terry Clark

Staff: County Administrator Coates, Superintendent Iosue, Finance Director Trombly, EMS Chief Spain, MNH Facilities Director Harrison, IT Director Hummel, Sheriff Rivera, HR Director May, County Project Manager Bouchard, and Executive Assistant Gouger

Guest(s):

At 8:34 AM, Commissioner Wozmak, Englund, and Clark responded as "present."

Public Comments

Upon recognition from the Chair, a Public Comment on topics of interest may be made, at most three (3) minutes in length.

I. Elected Officials & Department Head Updates

To receive, as informational, departmental updates requiring Commissioner review, participation, approval, and impactful departmental and operational issues.

Sheriff Rivera was recognized and said a tentative date is set for May 22 at 11:00 AM to meet with NH Department of Safety Assistant Commissioner Eddie Edwards, Homeland Security Director Rob Buxton, and Department of Education (DOE) Commissioner Frank Edelblut to discuss the proposed school Guardian Program. Rivera said they agreed on the amendment and language to be presented to the state Legislators. Sheriff Rivera stated that \$1.5 million over two years is being requested, which will allow for hiring the guardians and support staff, equipment, and other necessary expenses.

Rivera said that the program will be a two-year pilot program. At the end of year two, the County will start looking at the long-term plan for sustaining the program. The state most likely will not be able to maintain the program due to the number of schools, and he said there would need support from the school districts.

The goal is to hire ten staff to start with area coverage, whose sole responsibility is school security, not discipline or law enforcement.

Cheshire EMS Chief Spain was then recognized and provided updates on staffing. There are 14 Paramedics, Five AMT staff, and 18 EMT staff. He anticipates reaching out to Scott Symonds to do a basic EMT program in the fall and potentially an advanced EMT program in the spring of 2024.

He noted that 803 calls for service have been answered since November 14, 2022.

II. Scheduled Items

Master Agenda Item #1083: Presentation of Generator Bid – B. Harrison

Action Expected: Vote to accept generator bid as presented by Maplewood Facilities Director Bruce Harrison.

Harrison said we had received four bids, Milton CAT, Cummins Sales & Service, Powers Guaranteed Services, and Power Up Generator Service. There was a discussion regarding costs, and Harrison recommends going with Powers Guaranteed Services, as they seem to have the best all-around bid.

Commissioner Clark moved to accept the bid presented by Powers Guaranteed Services for the project. The motion was seconded by Commissioner Englund, and upon roll call vote, the motion passed unanimously.

Harrison also mentioned that the capital expenditure plan for the wastewater treatment plant repairs initially budgeted for \$3,500 had experienced a price increase of roughly \$1,000. However, it will still be under the approved budget of \$5,000 but Harrison wanted to ensure everyone was aware of the increased cost.

Master Agenda Item #1084: IT Semi-Annual Report – R. Hummel

Action Expected: To serve as a six-month informational report from IT Director Rob Hummel.

Hummel provided the following written report and spoke to each section.

IT Department Status Report - May 3, 2023

Summary

Staffing: All FTE positions are filled, and two trainees started in January.

Workload: Support demands are increasing with additional staff and county expansion. Several major vendor-driven upgrades are in progress for completion this year.

Cybersecurity: No known incidents of compromise. Direct attacks and probes are steady at approximately 500,000 per day. (183 million per year)

Operational Costs: Due to inflation, vendor support costs continue to rise significantly (10-20%). Hardware costs rising 50-100%.

Equipment Availability: Used equipment supply is drying up. Supply-chain delays for new networking equipment are hampering projects; lead times approaching 6 months to one year.

Staffing & Workload

For more than a year, the IT Department experienced extreme difficulty recruiting candidates for an existing vacancy. To address this, I restructured the department job categories to provide additional promotional steps as well as create a new "trainee" grade. This allowed us to hire candidates with less experience than would have been required for a higher grade. The strategy was successful and we filled both vacancies in January with support-level trainees.

The task list for IT staff continues to expand. Major drivers for the increased support requirements and additional workload are:

- Escalation of cyber-attacks, including phishing and email compromise
- An increase in the number of mobile/VPN users (connected families)
- A need to support multiple desktops per user (work from home)
- Large employee turnover (connected families, EMS, HOC)
- Software end of support-driven upgrades (Windows Server 2012R2, PBX)
- Purchasing driven by EMS and connected families
- Increase in system monitoring for malware/ransomware
- IT infrastructure upgrades
- Increased demands for vendor support (direct and indirect)

In addition, all aspects of the IT operation are under constant review and revision to keep pace with changes in best practice, anticipate new threats, and increase resilience. All staff members perform a wide range of activities including routine monitoring and maintenance, user support, and active research and development.

Cybersecurity - Perimeter

Maintaining a healthy cybersecurity posture continue to be one of the most challenging and impactful functions of the IT Department. To date, we are holding our own against attacks both on our data infrastructure and on our users.

Recently, new threats have emerged and are trending. Malactors are creating compromised websites that download malware when the site is accessed. Using SEO (search engine optimization) services, the malactors are elevating their compromised sites to the top of search results using phony keywords. Thus, a Google search for "best new golf drivers" may return a top result labeled "Best New Drivers 2023" but actually goes to a malware site. Because of people's tendency to click the first link, this approach often yields results.

Another emerging threat comes from "supply chain" or compromised cloud services. Instead of attacking companies directly, malactors target providers of cloud businesses that service those companies. Last month, it was revealed that a Chinese hacking group compromised the site of a popular messaging app. Victims who use the app were tricked into installing malware disguised as updates to the app. Most of these users were in NGOs and the attack affected users world-wide.

In another supply chain case, an employee at 3CX (a phone service provider) downloaded a stock trading program onto his business PC. The program was infected and allowed North Korean hackers to use the PC to gain access to the 3CX corporate network. They then installed malware in the phone system program code that 3CX provided to its customers. The result was that every user of the phone product had their devices compromised, granting the original attacker's remote access to their businesses.

There are two important lessons in these examples. First, prohibiting the unauthorized installation of programs or apps without IT involvement is critical to preventing compromise of workstations and other devices – regardless of the perceived convenience. This includes browser extensions for playing music, trading cryptocurrency, and social media. Second, allowing "cloud service providers" unrestricted access to the county network represents a significant risk, despite their claims otherwise.

Cybersecurity - Email

By its nature, our email system must accept connections from unknown sources. We use several techniques to reduce our exposure – and thus our vulnerability.

Geo-blocking: Refusing connections from roughly 98% of the countries in the world reduces the volume of incoming malicious emails significantly. Nonetheless, attacks via email originating from servers in the US and Canada pose a significant security challenge.

Sender Screening: This manual technique blocks emails based on the sender address (actual or faked). Many established domains are used expressly for delivering "spam" or infected emails. Some examples of blocked top-level domains include those ending in ".party" or ".vip". Specific domains that are known to have been compromised are also blocked, such as "glowormautocentre.co.uk".

Host Screening: This manual technique is similar to sender screening, but blocks email based on the name of the sending email server rather than the email address being used. Servers that identify themselves using numbers instead of a name or use non-visible characters in the name, for example, are typically malicious.

Dynamic Screening: The mail server program tracks failed login attempts or attempts to send to invalid addresses. If attempts exceed a set threshold, the server will automatically add the sender to a temporary block list. Each subsequent offense extends the time that the sender is blocked. This process has to be monitored to ensure that legitimate addresses are not blocked unintentionally as is often the case when county employees attempt to set up email on their phones.

Attachment Screening: Attaching documents to emails is a popular method for exchanging information. It is also widely employed to distribute malware or malicious links. The email server specifically prohibits certain file types from being delivered. This causes some level of inconvenience when attachments are blocked. Often, the problem occurs because the sender creates a document in an "incorrect format," such as a Word document that includes macros. Recent changes in the way some organizations send notification of encrypted mails has caused a significant problem in this regard.

Content Filter: The content of an email message can be examined in great detail, including the sender, recipient, subject, and body of the message. Our content filter detects common scams and puts the messages aside for manual examination. Emails contain phrases such as "change my direct deposit information" or "mystery shopper" or "Norton team" are often sent from recently-created gmail addresses and contain either malware or links to malware sites.

Cybersecurity – Patch Management

Installing security patches to both software and hardware continues to be a critical part of our infrastructure maintenance. Every patch must be researched, evaluated, and tested before we release it to the network. As often as not, the patch will unintentionally break some other function in the network. In addition to Windows patches, patch management is required for server hardware, network switches, firewalls, non-Windows servers, VPN clients, and more.

Unfortunately, patch management increases operational stress because the flaws they address are often severe and the time to react is short. Critical vulnerabilities may already be being actively exploited in the wild implying that the patch window is small. Up to 60-percent of breaches are ultimately attributed to unpatched vulnerabilities – where patches were available but simply not installed or were installed after a breach.

Cybersecurity - Assessment

Included with this report are excerpts from the April 30, 2023 Cyber Hygiene Assessment provided by CISA/DHS. This analysis of our external-facing systems is performed weekly. The latest assessment gives us a mostly clean bill of health. Most of the vulnerabilities noted are inconsequential because the systems are not configured in a way that exposes those faults (such as no public-facing connection, for example). The HVAC system continues to be the least secure as it is the responsibility of the vendor.

IT Department Projects

1. HOC Security System Update

The update to the "card reader" system at the HOC is mostly complete. The new hardware and software was put in place over several days. There was minimal disruption to the jail's operation. We are waiting on additional hardware to be delivered and training to be conducted. (Vendor contract.)

2. Maplewood WiFi Upgrade

The Aruba hardware infrastructure that provides WiFi at Maplewood was originally installed in 2016. The access points (APs) in use were not sold after 2018. Since that time, we have expanded and maintained the network by purchasing used equipment to minimize costs. Software security patches for the current system will cease in 2023. The new system will support enhanced capability, management, and security. We are waiting on hardware availability from an order placed over six months ago. (Vendor contract.)

3. Dispatch Workstations

The current dispatch workstations have reached the end of their useful service period. To support future operations, new workstations will be purchased and configured to support this role.

4. Jail Inmate Management System End-of-Life

The current IMS will go end-of-life in 2025 when the vendor abandons the project. IT is assisting HOC staff in evaluating replacement software from a security and business continuity perspective.

5. Time and Attendance Software

The current Kronos system will be end-of-life in the near future. IT is available to evaluate replacement systems.

6. Phone system update

The current version of our phone system reaches end-of-life this year. An upgrade is available that can be installed at no cost to the County. Plans are being made to test and configure this system before deployment to ensure continuity of service.

7. Windows Server Upgrade

The current server operating system version (2012R2) reaches end of support in 2023. All servers will have a new version (Server 2022) installed. This requires installation and configuration of the virtual hosts as well as upgrade of the virtual machines that run the County's critical business applications, including electronic charting, finance, inmate management, file shares, and dispatch. Every application must be ported to 2022 and vetted thoroughly before the switch is made.

8. Campus 10G Backbone Upgrade

To accommodate increased network traffic, the network backbone on all campuses is slated to be upgrade from 1Gbps to 10Gbps. The fiberoptic cabling in place was designed to support this upgrade; no rewiring will be required. The project will require upgrading selected convergence points in the networks to create the new backbone. Equipment is being purchased as needed when available inexpensively.

9. Enterprise Business Availability Redesign

The IT Department's availability, backup, and continuity (ABC) plan for the County was appropriate for our needs when first implemented eight years ago. It has been updated periodically as the environment has evolved. Today, the volume of data produced and used by County operations has increased to the point where traditional recovery methods create an unacceptably "return to service" time. In this redesign, the IT Department will design and implement several methods of increasing resiliency, including warm-site failover and continuous backup.

10. Cybersecurity Infrastructure Enhancements

IT continues to enhance its internal security information and event monitoring (SIEM) systems. These systems, implemented at no capital cost to the County, provide real-time analysis of security alerts generated by applications and network hardware at the perimeter. In 2023, a parallel system will be implemented to monitor and manage internal network activity. This new system will focus on internal threat detection, ransomware detection, and data leak prevention.

Respectfully Submitted,

Robert L. Hummel
Director of Information Technology

III. County Administrator

Weekly Operations Report - The County Administrator will update the Commissioners on activities that have taken place since the previous meeting.

Coates said that he was informed that as of yesterday at 11:59 PM, Diluzio was no longer an operating company, and they had moved forward with a plan to turn over their EMS coverage to Rescue, Inc from Brattleboro, Vermont.

Coates said that the City of Keene hosted a meeting with the towns under contract with Diluzio and had failed to contact the County and Cheshire Medical Center regarding the meeting.

Coates said it is up to the towns to make individual decisions regarding their contracts with Diluzio, now Rescue, Inc., and that each town select board makes that decision independently. He said that he was told that Rescue, Inc will house two ambulances in Keene, one at the Central Station and one at the West Station.

Coates said that he is now interested in telling the County's side of the EMS story and wants to get a timeline of events together to portray them as they occurred accurately. He stated that he is waiting to hear if the signed Non-Disclosure (NDA) is still valid now that Diluzio as a company is defunct from an attorney was involved in creating the original document.

Coates said that he also plans to address the negative comments that are now going around regarding Cheshire EMS operations and employees.

Coates said that the new Director of Nursing at Cheshire Medical has been doing a great job and that she was very pleased that twelve runs were completed for the hospital in one day and that they all ran smoothly.

Coates said that the Union Leader article regarding Cheshire EMS was positive, accurate and well-balanced. [Cheshire County launches its own ambulance service, gets pushback from Keene Fire | Health | unionleader.com](#)

Coates said that as of yesterday, roughly 80-90% of the speakers are lined up for the New Hampshire Association of Counties (NHAC) conference in October.

Coates said that he would like to move forward with the Coordinated Transportation Services CTS New Hampshire Medicaid document for the County to do non-emergency advanced life support (ALS) and Basic life support (BLS) transfers. Finance Director Trombly spoke briefly on the document, explaining that it is necessary. The Commissioners agreed it is important to complete the document and move forward with services to the County communities.

Coates discussed the dedication to the 2022 Annual Report that is being prepared, and Commissioner Wozmak would like to review this topic further at next week's meeting.

Coates said that Sheriff Rivera was notified that the incident simulation software and equipment he applied for had been approved for consideration in the final congressional budget.

IV. Old Business

Commissioner Clark then discussed needing to find a place to hold a public forum for the startup of Cheshire County Community Power (CCCP). The meeting is tentatively scheduled for May 24 and will be the introductory informational meeting for Cheshire County Community Power. The amendments must go through the Community Power Coalition of NH (CPCNH) Risk Management Committee and will receive final approval on May 22 at the CPCNH Annual meeting. The Commissioners will then approve the modified County Electrical Aggregation Plan (EAP).

The current plan is to hold the public forum at the County Hall building in the Commissioners Conference Room on the afternoon of the 24th at 2:00 PM.

V. New Business

VI. Consent Agenda Items:

Vote to accept the Weekly Manifests for May 3, 2023, and the meeting minutes of April 26, 2023.

Commissioner Clark moved to accept the manifests of May 3, 2023, and the minutes of April 26, 2023, as presented. Commissioner Englund Seconded the motion, and upon roll call vote, the motion passed unanimously.

VII. Calendar

Action Expected: To accept the calendar as informational and to make necessary changes/additions.

No changes.

VIII. General Discussion for Commissioners

Master Agenda Item #673: Commissioners - State Cost Shifting Letter and Restorative Justice Program

IX. Nonpublic Sessions: None

X. Adjournment

At 11:24 AM, Commissioner Englund moved to adjourn the meeting. The motion was seconded by Commissioner Clark, and upon roll call vote, the motion passed unanimously.

Recorded and edited by:
C. Gouger
Executive Assistant
Office of the Commissioners

Reviewed and submitted by:
Terry Clark
Clerk, Board of
Commissioners