In relation the audit findings pertaining to DR -disaster recovery, attached is the report with the responses therein. From yesterday, I also mentioned the timeline of both the audit and DR planning with contracted vendor TetraTech, as follows:

- **DR Timeline**

1. 12/2018 - Initiated TetraTech procurement for DR plan. Paid for out of grant that originally created COOP COG plan
2. 01/2019 – Completed BAC and Leg procurement approval for DR/TetraTech
3. 03/2019 – DR/TetraTech kickoff meeting
4. 04/2019 – Audit of IT started
5. 06/2019 – D/TetraTech onsite interviews – Audit invited
6. 08/2019 – Audit report completed/distributed
7. 09/2019 – Draft DR report distributed
8. 10/2019 – Draft DR report presentation to BC Exec and Leg.
9. 11/2019 – Create DR related project list for 2020 and beyond

In relation to the IT Security questions and responses, here is the summary list:

- **IT Internal – IT Security related due-diligence:**
    - County-wide multi-factor authentication
    - County-wide training for employees to prevent similar future incidents.
    - County-wide email migration to O365 and its built-in security features.
    - Continuing/on-going maintenance upgrades – regular habit and due diligence
    - Exploring shared services & reciprocities (locations, equipment, software, joint buys) with municipalities & SUNY Broome
    - Working on a Priority Task List of 12 tasks/projects
    - Contracted vCISO/IT Security Services (via Sirius vendor) for the remainder of the year for services that includes:
        - Ongoing security governance - consult with the client on the management and on-going development of the enterprise security program with regard to the NY regulations and other applicable security/compliance frameworks including: NIST CSF, Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA).
        - Security Posture Assessment - conduct an organization and information criticality workshop including high-level architecture and countermeasures review.
        - External Security Reviews – review and advise on methods hackers use to breach organizations without exploits.
        - Internal Periodic Reviews – including:
            - 1. Information criticality identification and risk discovery
            - 2. Design and configuration review
            - 3. Technical Vulnerability analysis
            - 4. Enterprise Security Governance Plan review
            - 5. Enterprise Security Policy review

        - Governance Risk and Compliance - enterprise governance and risk management to prepare for security audits and assessment of contractual obligations related to security management
        - Business Continuity and Disaster Recovery Analysis and Recommendations - Determine RTOs (recovery time objective as per COOP COG) and RPOs (recovery point objective as per dept requirement) for primary business systems and critical ancillary systems. Analyze capability to bring business processes and systems back on-line during an emergency with or without infrastructure staff to assist.
        - Incident Detection and Response Recommendations - analyze the existing resources and processes for incident detection and incident response. Based on this analysis, be able to provide detailed and actionable recommendations to both improve the incident response capability and effectiveness. Also provide "lessons learned" and field experience in incident handling to make process and procedure recommendations that have proven to be effective in the field.
    - Compiling a list of Cyber Incident Findings & Follow up task list that will be worked on now and into 2020