Homeland and Cybersecurity Update

Town Council Regular Meeting
July 8, 2025

Warrenton OEM: Independent & Recognized

- **Office of Emergency Management (OEM):**
  - Dedicated to Town-specific emergency preparedness & response.
  - Streamlined organization for rapid, effective action.
- **VDEM Recognition (April 2025):**
  - Officially recognized as an **independent Emergency Management Agency** by Virginia Department of Emergency Management.
- **Five-Year Achievement:**
  - Culmination of a robust, five-year effort.
  - Established a strong, independent emergency management jurisdiction within the Town

Collaborative Security: EM, Police & IT

- **Integrated Approach:** Effective Homeland Security relies on seamless coordination between these key departments.
- **Emergency Management:**
    - Leads overall preparedness, response, and recovery efforts.
    - Relies on Police for on-the-ground security and IT for communication/data.
- **Police Department:**
    - Provides law enforcement, incident response, and physical security.
    - Leverages IT for intelligence, communication, and digital forensics.
    - Works with EM on incident command and public safety.
- **Information Technology (IT):**
    - Secures critical infrastructure, networks, and data.
    - Enables secure communication for EM and Police during crises.
    - Provides tools for threat intelligence and cyber incident response.
- **Shared Goal:** Protect citizens, critical assets, and maintain operational continuity against all threats.

Interagency Information Sharing & Classification

- **Crucial for Security:** Effective Homeland Security depends on seamless, secure information exchange across Federal, State, and Local levels.
- **Data Classification Levels:**
  - **Unclassified:** Publicly releasable information.
  - **For Official Use Only (FOUO):**
    - Unclassified, but sensitive.
    - Not for public release; requires safeguarding.
    - Protects privacy, proprietary info, or law enforcement-sensitive data.
  - **Classified (Confidential, Secret):**
    - Information that could cause damage to national security if disclosed.
    - Strict access and handling protocols.
- **Ensuring Proper Handling:** Classification dictates who can access, share, and store information, safeguarding sensitive data while enabling necessary collaboration.

INTERAGENCY INFORMATION SHARING

DEPARTMENT OF INFORMATION TECHNOLOGY

IT Overview

The Town is continuing its proactive cybersecurity initiative to strengthen our defense posture, safeguard sensitive data, and ensure continuity of government services. This initiative reflects our long-term commitment to protecting critical systems and upholding public trust.

Our approach emphasizes:

- A layered defense strategy to mitigate evolving threats
- Responsible data stewardship and secure information sharing
- Controlled access to sensitive systems and services
- Alignment with national and state cybersecurity standards
- Ongoing readiness to detect, respond to, and recover from incidents

This strategic focus ensures the Town remains resilient and adaptive in an increasingly complex digital environment.

Current Cybersecurity Threat Landscape

Homeland Security alerts:

- Ransomware targeting local governments
- Increased phishing (geopolitical ties)
- Critical public sector software vulnerabilities

Relevance and Our Response

Why it matters: Highlights need for vigilance, modernizations, and layered security

Staff Objectives:

- Summarize federal alerts
- Review Town's readiness
- Outline integrity measures taken – including hardening of Town systems and networks

IT Data Security & Compartmentalization Strategy

The Town is continuing its ongoing review and progress in strengthening data security through structured access and oversight:

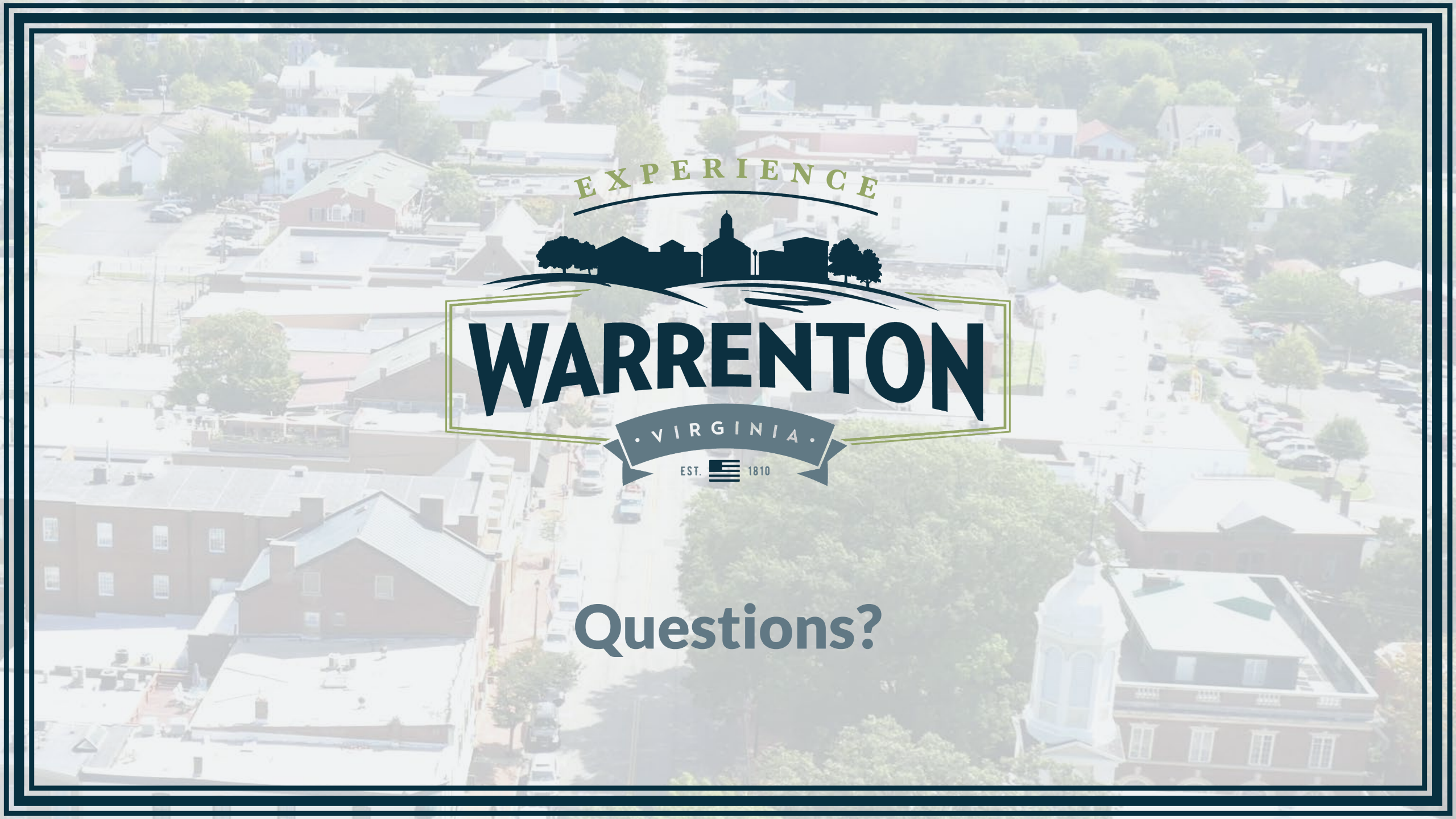
- **Data Classification**
- **Compartmentalized Access (Least Privilege)**
- **Role-Based Access Controls (RBAC)**
- **Audit & Monitoring**

Key Principle: Protecting Data by Limiting Access

Rather than over-securing individual files or accounts, our approach is to **protect the entire environment by ensuring data access is controlled and traceable.** Keeping sensitive information compartmentalized—and only accessible to those with a legitimate need—adds resilience against both accidental and malicious breaches.

INTERAGENCY INFORMATION SHARING

DEPARTMENT OF INFORMATION TECHNOLOGY



Questions?