City of Frederick 2025 Cybersecurity TTX

The City of Frederick, Maryland

EXERCISE & TRAINING

PROJECT DETAILS

DIFFICULTY: Medium

COST: $25,000

TIMEFRAME: 3 Months

DELIVERABLES: A four-hour cybersecurity focused Tabletop Exercise and After-Action Report/Improvement Plan

CORE COMPETENCIES:

- Cybersecurity
- Continuity of Operations
- HSEEP Exercise Planning
- HSEEP Exercise Facilitation
- After-Action Reporting
- Improvement Planning

PROJECT TEAM

Vision Planning and Consulting

CLIENT CONTACT

Nathan Hupp
Emergency Manager
Office of Emergency Management
City of Frederick
101N Court Street
Frederick, MD 21701
nhupp@cityoffrederickmd.gov
(301) 600-1495

PROJECT OVERVIEW

VPC was contracted by the City of Frederick, Maryland, to design and facilitated a four-hour, on-site, Homeland Security Exercise and Evaluation Program (HSEEP) Cybersecurity Tabletop Exercise (TTX) to test the City's Continuity of Operations Plan (COOP), and to develop an After-Action Report / Improvement Plan (AAR/IP) following the exercise.

PROJECT SUMMARY

The City of Frederick, Maryland, tasked VPC with designing and facilitating a Cybersecurity Tabletop Exercise (TTX) to test the City's Continuity of Operations (COOP) capabilities in response to a ransomware attack. The exercise brought together executive and departmental leadership, including subject-matter experts, to evaluate the City's preparedness, identify operational gaps, and gather lessons learned to inform future updates to the COOP Plan. The primary focus was on assessing how a cyber-attack (ransomware) could disrupt departmental systems, impact Mission Essential Functions (MEFs), and challenge the City's ability to maintain critical operations.

VPC staff developed all exercise and exercise communication materials, including exercise announcements and save the date communication materials; situation manuals; facilitator guides; slide decks; exercise evaluation guides; exercise feedback surveys; the after-action report (AAR); and identification of areas for improvement.

The exercise tested core capabilities such as operational coordination, communications, situational assessment, public information, and planning, specific to response and recovery. It explored key areas including notification of key entities, mandatory reporting requirements, alternative communication systems, information sharing protocols, public messaging strategies, and the identification and prioritization of MEFs. Through these focus areas, participants examined their ability to respond effectively to a cyber incident while minimizing operational disruptions.

The TTX was structured into three modules. The first module addressed detection and initial actions, focusing on identifying the attack and assessing immediate impacts on communication systems. The second module examined impacts on MEFs through breakout group discussions, where participants evaluated system disruptions, cascading effects, and strategies for maintaining operations during prolonged outages. The final module focused on restoration priorities, including decision-making around ransom payments, recovery timelines, and deactivation strategies.

The exercise provided participants with critical insights into system dependencies, restoration priorities, and interdepartmental coordination during a cyber incident. It also highlighted areas for improvement in communication strategies and situational awareness protocols. Ultimately, the exercise strengthened the City's preparedness for cyber threats and provided actionable recommendations to enhance future updates to its COOP Plan.

Following the exercise, VPC staff utilized the strengths, areas for improvement, and other observations by and comments by exercise facilitators, participants, and the client in order to develop a comprehensive After-Action Report and corresponding Improvement Plan.