INVESTMENTS IN INFORMATION TECHNOLOGY IMPROVEMENT & MODERNIZATION PROJECTS OVERSIGHT BOARD

Minutes
January 23, 2024

Call to Order and Roll Call

The first meeting of 2024 of the Investments in Information Technology Improvement & Modernization Projects Oversight Board was held on January 23, 2024, at 2:30 PM in Room 131 of the Capitol Annex. Representative John Hodgson, Chair, called the meeting to order, and the secretary called the roll.

Present were:
Members: Senator Gex Williams, Co-Chair; Representative John Hodgson, Co-Chair; Senators Cassie Chambers Armstrong and Max Wise; Representatives Chad Aull and Nancy Tate.

Guests: Mike Sunseri, Deputy Executive Director, Kentucky Office of Homeland Security; and David Carter, Chief Information Security Officer, Commonwealth Office of Technology

LRC Staff: Jennifer Hays, Adam Johnson, Sarah Watts, and Jennifer Smith.

Approval of Minutes

Upon motion by Representative Tate and second by Senator Williams, the minutes from the December meeting were approved without objection.

Next Generation 911 (NG911) Technologies

Mike Sunseri, Deputy Executive Director, Kentucky Office of Homeland Security, began with a quick overview of the 911 services board and its connection with the Office of Homeland Security. The 911 services board's roll is to collect and distribute wireless 911 fees. There are 117 certified PSAP's (public safety answer points). There are three types of subscribers which are postpaid, prepaid, and distribution formula where 97.5 percent of the fees collected go back into the local 911 services.

Mr. Sunseri continued by explaining the present and future of Next Generation 911 (NG911). With NG911, you will be able to send pictures, videos, and texts through a 911

call. In a NG911 environment, the call is routed using a geospatial routing system which saves time and could save lives.

The federal NG911 grant program gave $2.2 million in 2019 for foundational NG911 projects, and the state matched it at $1.4 million as required. The updates needed for the NG911 program are mapping and data display analytics, rapid deploy radius, aerial photography, and local GIS projects.

He continued by noting NG911 accomplishments: including new state road map, high resolution aerial photography, new monitors and workstations for data portal display, radius plus mapping, and (PSAP's) added to the statewide map. Mr. Sunseri added that 99 of 110 PSAP's have been published in the statewide database.

To move forward, IP connectivity for all certified PSAP's and geospatial call routing will be required. It is uncertain whether additional federal funding will be available. At this point, the 911 service's board has maxed out existing resources. The projected cost of funding NG911 is around $5 million per year.

Mike Sunseri, responded to Representative Hodgson's questions stating that the $5 million in the upcoming budget will get us to the next phase for NG911 by providing IP connectivity and the geospatial call routing.

Cybersecurity

David Carter, Chief Information Security Officer, Commonwealth Office of Technology (COT), began by explaining how COT builds their security programs. It begins with a mindset of a user, ends at the data, and is diligently applied every step in between. A combination of effective front line proactive defenses paired with comprehensive monitoring and response capabilities is necessary.

He continued by explaining a cyber security framework and the types of security. The cyber security framework includes these steps, identify, protect, detect, respond, and recover. There are two types of security. Traditional security is a fortress approach that relies on strong walls and boundaries to keep threats outside the protected enclave. Modern security must be intelligent, watching not only for bad things, but also good things behaving badly. The detection of, and response to, deviations from the normal and risky behavior is the new standard.

Mr. Carter continued by explaining the agency firewalls system which includes micro-segmentation, endpoint detect and response, and anti-malware. The intelligence of these firewalls understands that computers can talk to each other, so if the normal

becomes different, then the firewall will recognize that difference. Mr. Carter explained that of the cyber-attacks within the last 10 years, the majority included a phishing component. Phishing is a big threat, so COT does a phishing exercise every month for employees to stay up to date on phishing threats. State offices have seen a 78 percent decrease in phishing attacks, which is well below the national average.

Mr. Carter responded to Representative Williams' question by stating that providing an estimated cost of third-party penetration testing is challenging to do. He said they will have to look at the development of work and an outward assessment.

24 RS SB 63 - For Discussion Only

Senator Williams explained the name change being requested for the committee. ITOC, Information Technology Oversight Committee.

Adjournment

With no further business to come before the board, the meeting was adjourned at 5:16 p.m.