Department of Public Safety and Correctional Services
Concerns with HB 738/SB 705

The provisions of HB738/SB705 present significant challenges for the Department of Public Safety and Correctional Services (DPSCS), threatening to restrict critical access to federal criminal justice databases for both State and local law enforcement agencies. This could severely undermine criminal justice agencies' ability to protect public safety and effectively respond to criminal activity.

The DPSCS Information, Technology and Communication Division (ITCD) is the State Criminal Justice Agency. DPSCS ITCD hosts a multitude of systems designed to safeguard criminal history record information and criminal justice information for all State and various federal criminal justice agencies. DPSCS ITCD provides oversight of the Criminal Justice Information System - Central Repository (CJIS-CR), as well as the confidential electronic health records management system for incarcerated individuals. As the federally identified repository for State and federal criminal history record information/criminal justice information, the information technology services required to support the CJIS-CR are intricate, and the support of and access to this information is subject to State and Federal laws, regulations, and policies. Additionally, there is a significant amount of sensitive information that moves daily between operations, investigations, and technology personnel who support the information technology services; sensitive information that cannot be shared with anyone outside of a criminal justice agency.

The services provided by DPSCS ITCD are mission-critical, and the DPSCS infrastructure is designed to support such. This infrastructure consists of a series of networks, firewalls, mainframe systems, distributed systems, servers, video conferencing services, storage area networks, account management, and disaster recovery. These services and infrastructure must be available on a 24x7 basis to support DPSCS, criminal justice agencies and law enforcement in the State, and non-criminal justice agencies to aid in the furtherance of their duties.

Personnel accessing the aforementioned systems must undergo fingerprint-based background checks, pursuant to Federal regulation and policy. Additionally, these same systems are audited and certified by the Federal Bureau of Investigation and must maintain data storage and security compliance at the Federal and State levels. Specifically, criminal history record information, certain criminal justice information, confidential offender information, and sex offender information have legal requirements regarding its storage, maintenance, submission, dissemination, and/or publication.

DPSCS ITCD systems differ from most other systems in other State agencies in terms of their sensitivity and criticality. Without proper support and oversight by individuals who fully understand their function, dependencies, processes, laws, and other related issues, lives could be lost, investigations may be placed in jeopardy, operational security compromised, false arrests or imprisonments may occur, offenders may be improperly released, employers may hire

individuals that pose a risk to vulnerable populations, and many other serious consequences could occur.

MIDTPs are not static; they evolve and require ongoing enhancements throughout their lifespan to remain in compliance with legislative changes during the operations and maintenance phases. This highlights the need for the implementation team to stay involved throughout the entire lifecycle of the project, as they will have the most comprehensive understanding of the system's features and the impact of any changes. The systems managed by DPSCS are long-term and critical, as we serve as the State's repository for criminal history data.

Transferring responsibility for MIDTPs would create more obstacles. DPSCS ITCD is the better-equipped division to manage these projects, with the institutional knowledge and project management capabilities necessary to ensure success. The responsibilities of the information technology services managed by the DPSCS ITCD Chief Information Officer must be handled with great consideration.