STATE OF CONNECTICUT
Auditors of Public Accounts

AUDIT SUMMARY
Department of Correction
State Data Center General Controls

www.cga.ct.gov/apa

As of February 2023

BACKGROUND

The Department of Correction (DOC) oversees and administers fourteen operational facilities statewide currently housing approximately 10,000 inmates. In addition, the department maintains an administration division that oversees the various groups that support the department's statutory objectives.

As part of the department's administration division, the IT group oversees all aspects of computer-related operations. This includes administering staff computers, communications and networking, databases, and access to information systems and programs on behalf of agency staff and inmates. Collectively, this represents a critical function of the department and its continuous operation.

ABOUT THE AUDIT

We have audited certain operations of the Department of Correction in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to internal controls as of February 2023. The objectives of our audit were to evaluate the:

1. Department's internal controls over significant information technology resources;
2. Department's compliance with policies and procedures internal to the department or promulgated by other state agencies; and
3. Effectiveness and efficiency of certain management practices and operations.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Link to full report

6 Total Findings

Our audit identified internal control deficiencies; instances of noncompliance with laws, regulations, or policies; and a need for improvement in practices and procedures that warrant management's attention.

NOTEWORTHY FINDINGS

	Findings	Recommendations
1	Our review determined that while the Department of Correction maintains detailed procedures for many of the activities corresponding to the NIST control families (e.g., configuration management, contingency planning, maintenance, personnel security, risk assessment), it appears to lack high-level policy documents that govern these procedures.	DOC should ensure it maintains sufficient policies to mitigate threats to agency information technology assets and ensure compliance with regulations and laws relevant to its environment.
2	Our review noted the need for improvement to threat assessment procedures for DOC information technology systems, including potential sources of threats and expected responses.	DOC should improve its threat assessment procedures to address the criticality of assets, potential threats, and the likelihood of an adverse event compromising the confidentiality, integrity, and availability of those assets.
3	Our review uncovered the need for documented approval in the change management workflow. While DOC provided us with evidence that its information technology group uses software to place requests for changes, the department does not have a documented approval process that verifies that management was aware and accepted the implementation of the change.	DOC should establish a documented change management approval process.
4	In our review of the department's disaster recovery plan, we noted the absence of important elements necessary for the plan's optimum effectiveness, including prioritizing critical systems, identifying individuals responsible for conducting restoration, procedures to follow when necessary, and ensuring current copies of the plan are available at each recovery site. We also observed that personnel were not aware of the department's disaster recovery plan.	DOC should develop a comprehensive disaster recovery plan which enables staff to appropriately respond to disasters and ensures ongoing operational stability. The department should make the updated plan available to all appropriate personnel.
5	Our review of data center access procedures illustrated the lack of a formal documented approval process, or a regular review for removing unnecessary access. We identified individuals who do not have a job-based need to access the data center (e.g., executive staff, maintenance, and other non-IT staff members).	DOC should strengthen internal controls over granting access to the data center. Additionally, management should develop procedures to ensure formal periodic reviews of its access list to ensure that access is granted only to individuals who require it for the execution of their job responsibilities.
6	In our review, we noted that some of the Department of Correction's information technology systems are not current.	DOC should consider upgrading its outdated information technology systems whenever feasible to ensure operational stability and data security.