

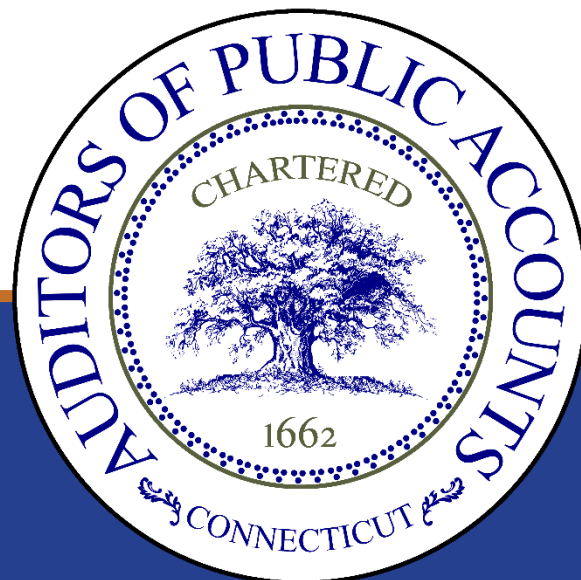
# AUDITORS' REPORT

---

## STATE DATA CENTER GENERAL CONTROLS

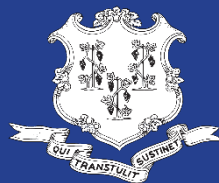
# Department of Public Health

AS OF JUNE 2022



**STATE OF CONNECTICUT**  
Auditors of Public Accounts

**JOHN C. GERAGOSIAN**  
State Auditor



**CLARK J. CHAPIN**  
State Auditor

# CONTENTS

---

INTRODUCTION.....	3
AUDIT-AT-A-GLANCE .....	4
STATE AUDITORS' FINDINGS AND RECOMMENDATIONS.....	5
Need for Updated Documentation (Planning) .....	5
Lack of Data Classification Assessment (Planning).....	6
Lack of Complete Risk Assessment (Planning) .....	7
OBJECTIVES, SCOPE, AND METHODOLOGY .....	9
ABOUT THE AUDIT .....	10

# STATE OF CONNECTICUT



## AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

STATE CAPITOL  
210 CAPITOL AVENUE  
HARTFORD, CONNECTICUT 06106-1559

CLARK J. CHAPIN

August 31, 2023

### INTRODUCTION

We are pleased to submit this state data center and general controls audit of the Department of Public Health (DPH) as of June 2022 in accordance with the provisions of Section 2-90 of the Connecticut General Statutes. Our audit identified deficiencies in internal controls, apparent non-compliance with policies and procedures, and a need for improvement in management practices and procedures that we deemed to be reportable.

The Auditors of Public Accounts wish to express our appreciation for the courtesies and cooperation extended to our representatives by the personnel of the Department of Public Health during the course of our examination.

The Auditors of Public Accounts also would like to acknowledge the auditors who contributed to this report:

Christopher D'Amico  
Jared Kolomyjec  
Joan Main

A handwritten signature in black ink, appearing to read "C. D'Amico".

Christopher D'Amico  
Principal Auditor

Approved:

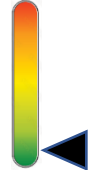
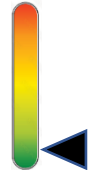
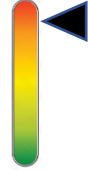
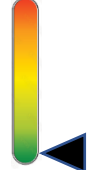
A handwritten signature in black ink, appearing to read "John C. Geragosian".

John C. Geragosian  
State Auditor

A handwritten signature in black ink, appearing to read "Clark J. Chapin".

Clark J. Chapin  
State Auditor

# AUDIT-AT-A-GLANCE

Category	Audit Risk	Description
<b>Maintenance</b>	 Low	Maintenance controls concern how well agencies keep their information technology (IT) systems up to date, patched, and operational. Our review noted that the Department of Public Health consistently monitors computer servers, keeps them up to date, and appropriately patches them. This engagement did not note any related findings or recommendations.
<b>Personnel</b>	 Low	Personnel controls identify how well the Department of Public Health's information technology group is staffed and able to perform its duties. Our review noted that current staffing levels appeared sufficient, and staff appeared knowledgeable. This engagement did not note any related findings or recommendations.
<b>Planning</b>	 High	<p>Planning controls indicate how well IT systems are insulated from disruptions to operations, unauthorized access, and similar activities that might have a detrimental impact.</p> <p>The Department of Public Health has not updated its Information Security Plan since June 2018. The Department of Public Health should periodically update and appropriately review its policies and procedures. (Recommendation 1)</p> <p>The Department of Public Health did not classify its information systems and data. The Department of Public Health should conduct a comprehensive data classification assessment in accordance with Office of Policy and Management policy. (Recommendation 2)</p> <p>The Department of Public Health has not conducted a complete risk assessment of its information technology systems. The Department of Public Health should conduct a comprehensive risk assessment for its information technology systems. (Recommendation 3)</p>
<b>Security</b>	 Low	Security controls identify how well the department's systems are protected (both physically and logically) and ensure its data are backed up and accessible. Our review noted that security over the Department of Public Health's information assets appeared reasonable. This engagement did not note any related findings or recommendations.

# STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our examination of the information technology (IT) general controls of the Department of Public Health disclosed the following three recommendations:

## Finding 1

### Need for Updated Documentation (Planning)

<b>Criteria</b>	Control CA-1 of the NIST Special Publication 800-53 recommends that policies and procedures should be periodically updated and reviewed.
<b>Condition</b>	The Department of Public Health has not updated its Information Security Plan since June 2018.
<b>Context</b>	The information technology environment changes rapidly. Therefore, agencies must ensure their policies and procedures reflect the most current information available, and by extension, minimize risk to normal operations.
<b>Effect</b>	IT operations may be exposed to a higher degree of risk from unforeseen threats and negative events.
<b>Cause</b>	Shifting priorities and placing new demands on IT staff appear to have contributed to this condition.
<b>Prior Audit Finding</b>	This finding has not been previously reported.
<b>Recommendation</b>	The Department of Public Health should periodically update and appropriately review its policies and procedures.
<b>Agency Response</b>	"We disagree with the finding. We acknowledge the importance of periodically reviewing and updating important guidance. That said, there are two important reasons why it didn't make sense for us to update the DPH's 2018 Information Security Plan at this time. First and foremost, the state is in the process of consolidating and optimizing information technology under the Department of Administrative Services (DAS). As part of optimization work, a new Security, Risk, and Compliance Division was created with a new Chief Information Security Officer and a new Deputy Chief Information Security Officer. The new division and leadership are working on

base information security guidelines for all agencies. It would not make sense for DPH to update its information security policies, procedures, or plans ahead of the base security guidance from the new Security Division. It is very likely that the base security guidance from the new Security Division will be sufficient guidance for DPH and obviate the need for department-specific guidance. Second, since the beginning of the pandemic, DPH has had to focus its attention on responding to the pandemic. IT resources had to create new information systems to support contract tracing and vaccinations, provide key information to leadership, and to enable a workforce of over 800 employees to work remotely. The Department prioritized its pandemic response work over updating its reasonably sufficient security guidance.”

**Auditors’ Concluding Comments**

Although we understand the need to prioritize and appropriately assign resources, the department should constantly ensure its policy documents remain current and relevant.

Although the Department of Administrative Services, Bureau of Information Technology Solutions is coordinating a consolidation and optimization of statewide IT resources, the department should work with its liaison to ensure it is properly safeguarding its operations and appropriately updating its policies and procedures.

## **Finding 2**

### **Lack of Data Classification Assessment (Planning)**

**Criteria**

The Office of Policy and Management (OPM) requires each executive branch agency to assign a classification to all data over which that agency has custodial responsibility. Regular data classification assessments ensure that statewide information technology resources are appropriately allocated for planning, system design and development, and necessary recovery operations. This affords state agencies a mechanism to better utilize resources and triage systems and data, thereby ensuring continued focus on assets from most to least critical.

**Condition**

The Department of Public Health did not classify its information systems and data.

**Context**

Each executive agency assigns a category and impact level to each data set in its custody, based on a federal data security matrix. The three federal security objectives (confidentiality, integrity, and accessibility) identify the parameters of an information system, and are matched with low, moderate, and high levels of risk for each objective. Completion of this exercise for each data set at an agency

ultimately establishes an overall criticality assessment, based on the most critical information system.

The department maintains numerous systems with various levels of criticality to agency operations. The data contained within some of these systems contains health-related and personally identifiable information (PII).

<b>Effect</b>	Lack of data classification could result in inefficiencies in assigning operational resources.
<b>Cause</b>	Noncompliance with this policy appears to be a lack of oversight by management.
<b>Prior Audit Finding</b>	This finding has not been previously reported.
<b>Recommendation</b>	The Department of Public Health should conduct a comprehensive data classification assessment in accordance with Office of Policy and Management policy.
<b>Agency Response</b>	"We disagree with the finding. We acknowledge the importance of a criticality assessment of data managed by DPH. To date, we haven't conducted such a criticality assessment because the cost to the department - which has numerous data systems - would be significant. In the past year, we received significant funding from the Centers for Disease Control and Prevention (CDC) to support a Data Modernization Initiative (DMI). As part of that initiative, we will gather relevant data and work with state's Chief Data Officer at OPM on the data criticality assessment."

## **Finding 3**

### **Lack of Complete Risk Assessment (Planning)**

<b>Criteria</b>	Control RA-3 of the NIST Special Publication 800-53 asserts that entities should conduct and document a periodic assessment of risk over its systems and data.
<b>Condition</b>	The Department of Public Health has not conducted a complete risk assessment of its information technology systems.
<b>Context</b>	A risk assessment of an agency's information systems and operating environment affords a greater ability for identifying, addressing, and preventing threats to its resources. A comprehensive assessment includes identifying the impact and likelihood of various risks across

all systems and devices, as well as the environment using and operating those systems.

<b>Effect</b>	The lack of a comprehensive current risk assessment could lead to an increased vulnerability to unforeseen threats and negative events for DPH information assets.
<b>Cause</b>	Increases in remote work demands and supporting ongoing systems have been prioritized over creating a risk assessment.
<b>Prior Audit Finding</b>	This finding has not been previously reported.
<b>Recommendation</b>	The Department of Public Health should conduct a comprehensive risk assessment for its information technology systems.
<b>Agency Response</b>	<p>"We disagree with the finding. DPH was not aware that there was a statute, regulation, policy, procedure, or other formal expectation that the agency should follow the NIST SP 800-53 federal guidance. In the Auditors of Public Accounts Agency Guide (2022), there is no mention that agencies should follow federal NIST guidance with respect to Information Technology work.</p> <p>Although we acknowledge that following the federal NIST guidance might provide some benefit to the agency and state, we suggest that this compliance would be costly, and we suggest that the costs should be evaluated against the benefits before committing the agency and state to additional costly compliance procedures."</p>
<b>Auditors' Concluding Comments</b>	Although there are no formal policies requiring a risk assessment, given the importance of DPH and its mission, the department should ensure it is able to appropriately define and respond to risks and events that could negatively impact its information systems and operations. Adoption of a security framework would allow the department to inform and direct its information technology decision making.



# OBJECTIVES, SCOPE, AND METHODOLOGY

We have audited certain operations of the Department of Public Health (DPH) 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 June 2022. The objectives of our audit were to evaluate the:

1. Department's internal controls over significant information technology functions;
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.

Our methodology included reviewing written policies and procedures and other pertinent documents; interviewing various personnel of the department; and testing selected transactions. Our testing was not designed to project to a population unless specifically stated. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We tested internal controls using the National Institute of Standards and Technology's (NIST) Special Publication 800-53 - "Security and Privacy Controls for Information Systems and Organizations" as a guide. This publication includes internal controls that provide a comprehensive foundation for an organization's information security. We used this publication to plan the testing performed for this engagement.

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.

The accompanying Agency Overview is presented for informational purposes. This information was obtained from various available sources including, but not limited to, the department's management and the state's information systems, and was not subjected to the procedures applied in our audit of the office. For the areas audited, we identified deficiencies in internal controls, apparent non-compliance with policies and procedures, and a need for improvement in management practices and procedures that we deemed to be reportable.

# ABOUT THE AUDIT

## **Audit Purpose**

We conducted this audit to obtain an understanding of the Department of Public Health's data center and its information systems and data. Our review was intended to: (1) identify the design and implementation of the department's IT general controls, (2) assess and evaluate those controls and practices against industry standards and state policies and procedures, and (3) identify and communicate opportunities for improvement in the department's IT control environment.

## **Agency Overview**

The Department of Public Health is a repository for and custodian of state residents' health information and vital statistics. The department provides personal health and wellness training and guidance, assists and educates pregnant mothers and new parents, promotes environmental health guidance, and conducts research and statistical analysis on multiple topics. Furthermore, it provides oversight and licensure for various practitioners including medical and dental professionals, caregivers, barbers, beauticians, and therapists. The department also maintains and operates a lab for testing infectious diseases, water supplies, and similar samples.