Evaluation of Information Technology Security at the Colorado Department of Transportation

Colorado Department of Transportation

Governor's Office of Information Technology

Information Technology Performance Evaluation

Public Report

February 2020

Eide Bailly LLC

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE
Representative Lori Saine – Chair
Representative Dafna Michaelson Jenet – Vice Chair
Representative Rod Bockenfeld
Senator Rhonda Fields
Representative Tracy Kraft-Tharp
Senator Paul Lundeen
Senator Jim Smallwood
Senator Nancy Todd

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Eide Bailly LLP	Contractor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT **WWW.STATE.CO.US/AUDITOR**

A BOUND REPORT MAY BE OBTAINED BY CALLING THE
OFFICE OF THE STATE AUDITOR
303.869.2800

PLEASE REFER TO REPORT NUMBER 1926P-IT WHEN REQUESTING THIS REPORT

EideBailly®

CPAs & BUSINESS ADVISORS

February 2020

Members of the Legislative Audit Committee:

This report contains the results of the Evaluation of Information Technology Security at the Colorado Department of Transportation. The assessment was conducted pursuant to Section 2-3-103, C.R.S, which authorizes the State Auditor to conduct evaluations and assess the security practices of information technology systems of all department, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Colorado Department of Transportation and the Governor's Office of Information Technology.

We conducted this engagement as an IT performance evaluation, and although we did not attempt to strictly follow generally accepted government auditing standards, we did obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and recommendations based on the evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

During our evaluation work, we identified certain matters that are not included in this evaluation report that were reported to the Colorado Department of Transportation and the Governor's Office of Information Technology management in a separate confidential report dated February 2020. These matters were considered sensitive to protecting state information technology assets.

E. Anders Erickson
Principal-in-Charge of Cybersecurity
Eide Bailly, LLC

CONTENTS

REPORT HIGHLIGHTS

Evaluation of Information Technology Security at the Colorado Department of Transportation

Involved assessment of IT security management and operations at both the Colorado Department of Transportation (CDOT) and Governor's Department of Information Technology (OIT)

Information Technology Performance Evaluation, 1926P-IT, February 2020

EVALUATION CONCERNS

By statute, Governor's Office of Information Technology (OIT) is the Information Technology Service Provider for the Colorado Department of Transportation (CDOT). However, CDOT continues to perform certain IT related functions for information systems managed by the Intelligent Transportation Systems (ITS) branch. In addition, OIT has not established the process and procedures necessary to ensure all CDOT personnel and OIT personnel supporting CDOT are trained and educated on their roles and responsibilities for ensuring the confidentiality, integrity, and availability of CDOT IT systems and data.

BACKGROUND

The Colorado Department of Transportation

- CDOT's mission is to provide the best multi modal transportation system for Colorado that most effectively moves people, goods, and information. CDOT has multiple divisions and programs. The evaluation included a review of seven information systems that help support CDOT's mission.

The Governor's Office of Information Technology

- OIT is the State's centralized Information Technology Service Provider responsible for managing information technology resources and staff for CDOT.
- OIT hosts and manages CDOT's information systems that were under review during the evaluation.
- OIT is also responsible for maintaining the State's IT Security Program and managing Colorado Information Security Policies and OIT Cyber Policy requirements at executive branch agencies, including CDOT.

KEY FACTS AND FINDINGS

- The ITS branch within CDOT has not consolidated IT property and IT employees to OIT.
- OIT has not established the process and procedures necessary to ensure all CDOT personnel and OIT personnel supporting CDOT are trained and educated on their roles and responsibilities for ensuring the confidentiality, integrity, and availability of CDOT IT systems and data.

RECOMMENDATIONS

- The Colorado Department of Transportation (CDOT) should address the non-consolidation of the ITS branch.
- The Governor's Office of Information Technology (OIT) should improve security training and awareness controls over CDOT systems and personnel.

CHAPTER 1
Overview

Colorado Department of Transportation

The Colorado Department of Transportation (CDOT or the Department) is responsible for operating and maintaining Colorado's more than 23,000 lane-mile state highway system, including more than 3,000 bridges, and maintaining the aviation system plan, under the policy direction of the eleven-member Transportation Commission. The Department's responsibilities also include managing highway construction projects, implementing the State's Highway Safety Plan, repairing and maintaining roads, providing technical support to local airports regarding aviation safety, and administrating the reimbursement of aviation fuel tax revenues and discretionary grants to local airports. To carry out its responsibilities, CDOT relies upon a broad range of information technology (IT) systems and applications that facilitate a broad range of mission-critical activities – from human resources to highway and tunnel operations and security.

In February 2018, a ransomware attack was launched on the Department's network and information systems. This attack encrypted departmental computers and data and the attacker demanded a ransom before they would provide the decryption key. In consultation with State and Federal authorities, the Department reported it would not pay the ransom. The attack forced 2,000 employees off their computers, and while system functionality was eventually restored, the restoration and cleanup efforts resulted in a cost of over $1.5 million.

Governor's Office of Information Technology

The Governor's Office of Information Technology (OIT or the Office) oversees executive branch department technology initiatives and services, including enterprise application management and support, database management, network security and management, communication technology services, data center operations, information security, help desk services, public safety communications, procurement, project management, and IT economic development. Statute requires OIT to develop policies, standards, specifications, and guidelines for IT and related procedures to effectively and securely manage IT [Section 24-37.5, C.R.S.]. The implementation of this statute also required the transfer of all IT property and IT employees from executive departments to OIT. Accordingly, much of the management and operational activities for CDOT systems are currently conducted by OIT. However, the Department continues to maintain control of some of its mission-critical IT systems – specifically those managed by the Intelligent Transportation Systems (ITS) branch within CDOT.

Evaluation Purpose, Scope, and Methodology

The purpose of this IT performance evaluation was to determine whether CDOT and OIT had adequate information technology and systems security practices in place to protect the confidentiality, integrity and availability of the CDOT IT assets, information, and data. During our evaluation, we assessed the IT systems and security practices that are overseen and managed by OIT – the Department's primary IT

service provider. Where the Department's IT systems and security practices were managed or operated by CDOT personnel, these were also included within the scope.

The scope of this IT security performance evaluation included the following activities: *Security Control Assessment*, *Social Engineering Assessment*, and *Security Vulnerability Assessment.* The scope and methodology for each of these assessments is outlined below.

The ***Security Controls Assessment*** consisted of an evaluation of the information security environment at CDOT in order to determine each organizations' adherence to the State's information security policies and leading industry standards or best practices, as outlined by the following National Institute of Standard and Technology (NIST) Special Publication (SP) 800-53 Revision 4:

Access Control (AC)
Awareness and Training (AT)
Audit and Accountability (AU)
Security Assessment and Authorization (CA)
Configuration Management (CM)
Contingency Planning (CP)
Identification and Authentication (IA)
Incident Response (IR)
Media Protection (MP)
Physical and Environmental Protection (PE)
Planning (PL)
Personnel Security (PS)
Risk Assessment (RA)
System and Services Acquisition (SA)
System and Communications Protection (SC)
System and Information Integrity (SI)

The testing methodology focused on areas of greatest risk to the Department and its systems. Test procedures were designed and executed to determine if appropriate IT security controls were implemented, operating as intended, and producing the desired outcome with respect to meeting applicable security requirements.

The ***Social Engineering Assessment*** was intended to evaluate the ability of targeted personnel to identify and appropriately respond to unauthorized attempts to access the Department's systems, applications, and networks. The methodology for this assessment utilized the same strategies that "malicious" attackers would use to gain confidential information. Specifically, mock phishing emails were distributed to all CDOT personnel and those OIT personnel charged with the management and support of CDOT systems and applications.

The purpose of these tests was to determine if personnel were susceptible to common phishing scenarios by assessing the participants' level of awareness and comprehension of phishing. These tests also ascertained the participants' understanding and compliance with State policies around handling e-mails containing links and/or attachments and their ability to recognize a questionable or fraudulent message.

The ***Security Vulnerability Assessment*** consisted of a series of technical tests to identify vulnerabilities in the implementation and configuration of CDOT systems, networks, and key applications. These tests included External Network Vulnerability Testing, Internal Network Vulnerability Testing, and Web Application Testing.

- External Network Vulnerability Testing – The objective of this testing was to establish a comprehensive view of the CDOT IT network as it appears from the Internet and to identify weaknesses within the network configuration that could allow unauthorized and/or

unsuspected access to the internal network. Accordingly, the focus of this exercise was the identification of potential security weaknesses in firewalls and gateway devices utilized to protect CDOT IT networks. Testing was conducted from the Internet on infrastructure managed by both CDOT and OIT. A combination of proprietary tools and utilities, commercial products, and publicly available open source tools were utilized.

- Internal Network Vulnerability Testing – The objective of this testing was to establish a comprehensive view of CDOT's internal network and to identify weaknesses in the internal network configuration that could allow unauthorized and/or unsuspected access to critical resources or the execution of unauthorized processes. The focus of this exercise was the identification of potential security weaknesses in CDOT network devices, servers, and workstations. Testing was conducted utilizing a combination of commercial products and publicly available open source tools and utilities.

- Web Application Testing – The objective of this testing was to identify web application vulnerabilities that may exist due to configuration or coding errors. Utilizing configuration information provided by OIT for key web-based applications, this testing mimicked attackers by exploring the applications and creating a list of potential application vulnerabilities. These potential vulnerabilities were then evaluated and verified. Testing was conducted utilizing a combination of commercial products and publicly available open source tools and utilities.

Please Note: The detailed results of the social engineering assessment and security vulnerability assessment, including the external network vulnerability testing, internal network vulnerability testing, and web application testing, were provided to CDOT and OIT management under separate confidential cover. The results included detail on the specific problems and vulnerabilities we identified during the assessment as well as related information that the agencies can use to remediate them. However, where applicable, within the findings of this report, we have included recommendations to assist OIT and CDOT with remediating the causes of the problems noted during the security vulnerability assessment.

CHAPTER 2
PUBLIC FINDINGS AND INFORMATION

INTELLIGENT TRANSPORTATION SYSTEMS

The Intelligent Transportation Systems (ITS) branch *(also referred to as "Traffic Operations" or "TOC")* is a branch within Colorado Department of Transportation (CDOT) consisting of IT personnel and IT equipment that works semi-independent of Governor's Office of Information Technology (OIT). During the consolidation of a majority of the state's IT personnel and IT equipment into OIT, CDOT business systems and infrastructure were transitioned to OIT; however, the ITS branch did not consolidate and continues to operate a data center and manage a suite of applications, databases, workstations, and servers. ITS does rely on OIT for performing data backups, providing access to the CDOT domain and email, developing and distributing security awareness training, and notifying ITS administrators of patch and system updates. Some of the most critical IT systems within CDOT are operated and managed by ITS. These include applications that facilitate or support traffic monitoring, weather stations, weigh-in motion (WIM), traffic signals, messaging signs, ramp meters, and traffic cameras.

What evaluation work was performed and what was the purpose?

To conduct our assessment and support our conclusions, we interviewed OIT and CDOT management and staff to understand the role of the ITS branch within CDOT and their relationship and reliance upon OIT. We reviewed ITS standard operating procedures. We examined state laws to understand the requirements for consolidation and the exceptions granted to non-consolidated agencies. Much of our control testing of OIT covered the people, processes, and technologies for ITS.

What problems did the work identify and how were the results measured?

The ITS branch within the CDOT has not transferred IT property and IT employees to OIT. ITS has not been granted an official exception to this consolidation requirement.

> *Senate Bill 08-155 as codified in CO Rev Stat § 24-37.5-104 (2018) transfers IT property, real and personnel and IT employees of all State agencies to the Office of Information Technology. "State agency" does not include THE LEGISLATIVE OR JUDICIAL DEPARTMENT, THE DEPARTMENT OF LAW, THE DEPARTMENT OF STATE, THE DEPARTMENT OF THE TREASURY, OR state-supported institutions of higher education.*

Why did the problems occur?

CDOT indicated that, when the consolidation occurred, the ITS branch continued to operate independently and did not transition IT equipment and personnel to OIT because ITS operates systems that are highly specialized and require a specific IT skillset to properly manage and maintain. CDOT did not feel that OIT has the necessary skillset and expertise to manage and secure their mission-critical systems. However, CDOT has not pursued legislative change to bring this structure into compliance.

Why do these problems matter?

The consolidation of all CDOT IT personnel and IT equipment into OIT with the exception of the ITS branch has resulted in confusion of responsibility for many of the IT controls in the ITS branch. As part of a consolidated agency, ITS should be relying on OIT for many security activities. By not consolidating with the rest of CDOT, ITS is left on its own and has neglected to implement some controls (e.g., configuration management and contingency planning). As ITS operates independently, OIT may not have purview into the following IT security activities within ITS:

- Configuration management and change control to the ITS network and applications.
- Access control to ITS specific applications, including user provisioning and deprovisioning.
- Management of ITS network infrastructure.
- Monitoring activities within the ITS network.

If ITS were consolidated under OIT, the activities listed above would be the responsibility of OIT. Furthermore, by not consolidating under OIT, the ITS branch within CDOT is not in compliance with statutory requirements, and therefore, may be operating in a way that does not realize the intended benefits related to consolidation efforts, such as operational efficiencies and cost savings.

RECOMMENDATION 1:

The Colorado Department of Transportation should evaluate the non-consolidation of the Intelligent Transportation System (ITS) branch and work with OIT to consolidate the ITS branch operations under OIT or develop an alternative to bring the ITS branch into statutory compliance. If CDOT works with OIT to consolidate the ITS branch, CDOT should work with OIT to develop a plan for the migration of all IT property and IT employees within the ITS branch to OIT. This plan should address the security, architectural, and personnel needs of ITS necessary to maintain mission-critical operations.

AGENCY RESPONSES:

COLORADO DEPARTMENT OF TRANSPORTATION

RECOMMENDATION 1:

Partially Agree. Implementation Date: May 2020. Management partially agrees with the recommendation to work with OIT and pursue a legislative change or other appropriate exemption but would not support any consolidation. ITS and related systems directly impact life safety and requires specialized support and transportation experience. The ITS systems directly impact tunnel, highway, traffic signals and operation of the entire transportation system. The life safety, criticality and uniqueness of operating the highway system are important for protecting the lives of our traveling public and harmonize with the rest of CDOT 24/7/365. Also, with the Ransomware experience, the ITS systems and security, protected and prevented at Statewide catastrophe because it was isolated from OIT's network and operations, and should remain separated for business continuity from the State level. We recommend seeking exception from the consolidation.

AUDITORS ADDENDUM: The issues identified in this finding address the need to adhere to the statute that requires consolidation or pursue an alternative to bring the ITS branch into statutory compliance as viable solutions to address this finding. Under the current operating arrangement, there is an increased risk of intentional or unintentional loss of confidentiality, integrity, or availability to CDOT information and/or resources because, as noted by the specifics of the issue, OIT may not have purview into key IT security activities conducted by the ITS branch.

Security Training and Awareness

The Governor's Office of Information Technology (OIT) develops and documents security training and awareness materials and disseminates these to CDOT and OIT personnel. The Office of Information Security (OIS) within OIT is responsible for ensuring all OIT personnel complete security training. In addition, OIS periodically distributes training materials to the Colorado Department of Transportation (CDOT). The CDOT Office of Employee Development receives training materials from OIS and is responsible for ensuring this training is completed by all CDOT personnel. CDOT provides training completion reports to OIT quarterly.

Security awareness training is conducted with each new user as part of the onboarding process. All users are then required to participate in security awareness refresher training annually. The annual training developed by OIS is broken down into modules that are distributed to users throughout the year on a quarterly basis. If an OIT employee does not complete the annual training, it will be noted on their performance evaluation.

What evaluation work was performed and what was the purpose?

To conduct our assessment and support our conclusions, we interviewed OIT and CDOT management and staff to understand the processes and practices in place for providing security training and awareness. We discussed training requirements for general users as well as role-based training provided to applicable OIT and CDOT staff. We reviewed security training and awareness materials developed and distributed by OIS. We tested training records for a sample of 20 current CDOT and OIT personnel to determine compliance with applicable state policies. We also conducted simulated email phishing attacks on 3,522 CDOT and OIT personnel to ascertain their ability to identify and recognize malicious emails.

What problems did the work identify and how were the results measured?

We identified the following problems at OIT regarding security training and awareness:

1. Contractors with access to CDOT systems and data are not tracked to ensure they complete security awareness training, either when initial access is granted, with system changes, or annually.

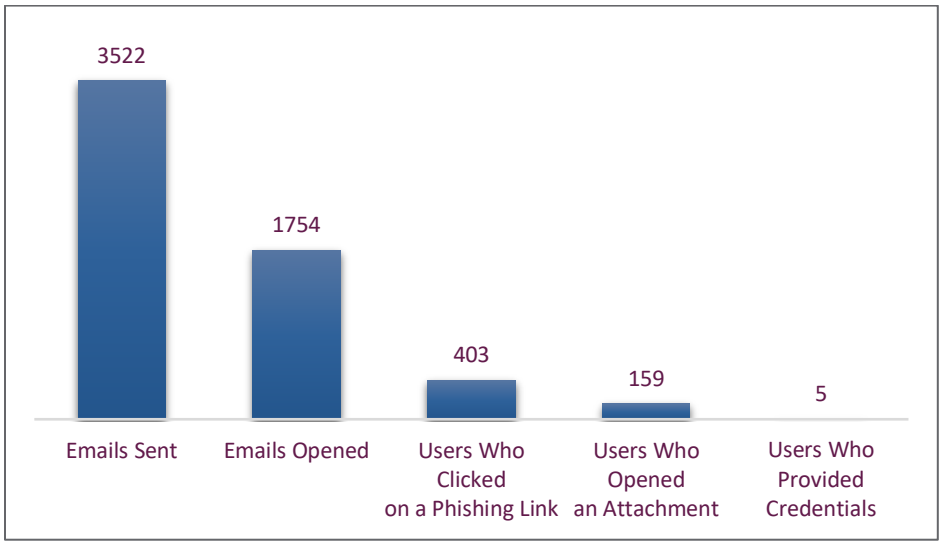
   CISP-002 Section 9.1.3 Security Awareness Program & Training - OIT is required to in consultation with and when required by the Business Owner, provide basic security awareness training to all information system users (including, but not limited to, managers, senior executives, and

contractors) as part of initial training, when required by Information System changes, and annually thereafter.

2. Formal role-based security training for OIT personnel or business owners who have key security responsibilities has not been developed.

   CISP-002 Section 9.2.1 Role-Based Security Training - OIT is required to provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes, and annually thereafter.

3. Our simulated phishing attacks resulted in 562 users that either clicked on a link or attachment within an email that we had sent them. The complete report of our simulated phishing attacks can be found in our Social Engineering Report provided to management under separate confidential cover. The diagram below provides an overview of the results of our simulated phishing attacks.



   Analysis of the results of these exercises identified the following areas of concern:

   - Twenty-seven OIT users that received simulated email phishing attacks clicked on a link or opened an attachment.
   - Two of the twenty-two CDOT users with local administrative access that received simulated phishing attacks clicked on a link or attachment.

   The Center for Internet Security (CIS) Top 20 Critical Security Controls is a prioritized set of best practices created to stop the most pervasive and dangerous cyber threats. Control number 17 on this list is entitled – Implement a Security Awareness and Training Program. The second of two main points describing this control states, "Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls."

4. Formal sanctions have not been established and enforced for individuals who fail to complete the required security awareness training in a timely manner.

CISP-012 Section 9.7.1 Personnel Sanctions - OIT and Business Owner shall employ a formal sanctions process for individuals failing to comply with established information security policies and procedures.

CISP-002 Section 10 Compliance - Failure to comply may result in the Chief Information Security Officer temporarily discontinuing or suspending the operation of the solution and/or resource until such compliance is established as deemed solely by the Chief Information Security Officer.

Why did the problems occur?

A OIT has not established procedures for coordinating with CDOT to identify and train CDOT contractors.

B OIT has outlined security roles and responsibilities for OIT and Business Owners but has failed to properly identify and educate those users on their expectations. OIT had not provided an additional explanation for why they have not provided role-based security training.

C OIT has not provided an explanation for not following up on user security awareness training within CDOT to ensure all users are properly trained on their cyber security responsibilities.

D OIT has not expanded its training and education initiatives to include regular email phishing campaigns of users with access to state systems and data. OIT has not provided an explanation for why they have not conducted regular email phishing campaigns.

Why do these problems matter?

Educating users on their cyber security responsibilities is critical to ensuring the reliability and protection of state information systems and data. Role-based security training for all personnel who conduct security-related functions is also an essential activity to successfully implement critical security controls. Without this training, staff may not be aware of the current security requirements and therefore may not implement the requirements. Without effective training and awareness on current social engineering threats and attacks (i.e., phishes, ransomware attacks, etc.), users may also not be aware of these threats and how to handle them to mitigate or prevent them from exploiting IT environments, systems, or data.

RECOMMENDATION 2:

The Governor's Office of Information Technology (OIT) should improve security training and awareness controls over CDOT systems and personnel by:

A Collaborating with CDOT to establish a program for the management of contractors with access to CDOT systems and data. The information from this program should then be used to ensure compliance with organizational requirements for security training and awareness.

B Developing role-based training for all individuals that have specific roles and responsibilities outlined within organizational information security policies.

C Establishing and enforcing sanctions for individuals who do not complete security awareness training in a timely manner and working with CDOT to implement the formal sanctions process for individuals failing to comply with established information security policies and procedures.

D Conducting regular, practical exercises in security awareness training that simulate actual cyber-attacks (e.g. performing email phishing of users regularly).

AGENCY RESPONSES:

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

RECOMMENDATION 2:

A. **Agree. Implementation Date: August 2020**. The Governor's Office of Information Technology (OIT) agrees with this finding. OIT will collaborate with The Department of Transportation to ensure organizational compliance for security awareness and training.

B. **Agree. Implementation Date: December 2020**. The Governor's Office of Information Technology (OIT) agrees to this finding. OIT is developing Cyber Policy Training and will provide this training to all OIT employees. In addition, OIT will create a version of the training that will be applicable to CDOT personnel and will be provided to CDOT personnel who perform IT functions.

C. **Agree. Implementation Date: December 2020**. The Governor's Office of Information Technology (OIT) agrees with this finding. OIT will establish and enforce a Sanctions policy for OIT employees who do not complete security awareness training in a timely manner. Once implemented at OIT, OIT will provide this sanctions policy to CDOT with a recommendation to implement this or a similar policy at CDOT.

D. **Agree. Implementation Date: September 2020**. The Governor's Office of Information Technology (OIT) agrees with this finding. OIT will begin phishing emails and conduct a tabletop exercise with The Department of Transportation on a regular basis.

Glossary

Access Control

Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Critical System

Systems that provide critical data to the public, and serve a vital function to government, but do not affect life-safety and must be recovered within 72 hours to a week of a system failure.

Executive Branch Agency

All of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

System

For the purpose of this evaluation, a "system" is the collective sum of an electronic computer application, as well as its accompanying operating system and database.

System Security Plan

Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.