



Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued September 5, 2018

Administration of the Internet of Things

For the period July 1, 2016 through March 31, 2017





Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

September 5, 2018

Mr. Curtis Wood, Secretary
Executive Office of Technology Services and Security
1 Ashburton Place, Eighth Floor
Boston, MA 02108

Dear Mr. Wood:

I am pleased to provide this performance audit of the administration of the Internet of Things at various state agencies. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2016 through March 31, 2017. My audit staff discussed the contents of this report with management of the Executive Office of Technology Services and Security, whose comments are reflected in this report.

I would also like to express my appreciation to the Executive Office of Technology Services and Security and the Division of Capital Asset Management and Maintenance for the cooperation and assistance provided to my staff during the audit.

Sincerely,

A handwritten signature in blue ink, appearing to read "SMB", written over a light blue circular watermark.

Suzanne M. Bump
Auditor of the Commonwealth

cc: Carol Gladstone, Commissioner, Division of Capital Asset Management and Maintenance

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
OVERVIEW	3
AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY	8
DETAILED AUDIT FINDINGS WITH AUDITEE’S RESPONSE.....	11
1. The Commonwealth needs to take additional measures to ensure the effective and efficient adoption of Internet of Things technology.	11
a. The Commonwealth’s Enterprise Information Security Policy does not offer any guidelines to state agencies regarding the adoption of IoT technology.	11
b. The Commonwealth does not have a formally documented information security incident response plan.	12
c. The Division of Capital Asset Management and Maintenance did not involve the CCIO in a project that connected IoT devices to the Massachusetts Access to Government Network.	13
APPENDIX	17
PHOTOS	18

LIST OF ABBREVIATIONS

CBEI	Commonwealth Building Energy Intelligence
CCIO	Commonwealth's chief information officer
DCAMM	Division of Capital Asset Management and Maintenance
DEP	Department of Environmental Protection
DPH	Department of Public Health
DTA	Department of Transitional Assistance
EISP	Enterprise Information Security Policy
EOTSS	Executive Office of Technology Services and Security
IoT	Internet of Things
IT	information technology
MAGNet	Massachusetts Access to Government Network
MassDOT	Massachusetts Department of Transportation
MBTA	Massachusetts Bay Transportation Authority
NIST	National Institute of Standards and Technology
OSA	Office of the State Auditor

EXECUTIVE SUMMARY

The Internet of Things (IoT) is the interconnection of devices via the Internet to allow the devices to collect and receive data over a network without requiring human-to-human or human-to-computer interaction. The flow of information in the IoT relies on what are commonly referred to as “smart” devices or on sensors that can be found in many products such as thermostats, health monitors, and motor vehicles. These devices need to collect, respond to, and/or transmit data as part of their normal operations. The IoT has many beneficial applications. For example, IoT-enabled devices and equipment are used to manage traffic; monitor health, weather, and energy; sense changes in environmental conditions to make necessary adjustments to control costs; and monitor equipment failure to ensure timely repair. Some common IoT devices include fitness trackers; smart watches; health monitoring devices; environmental monitoring devices; and devices in vehicles, such as those for global positioning system location and autonomous driving. It has been estimated that about 30 billion devices will be connected to the IoT by 2020.

In this audit, we obtained an understanding of the Commonwealth’s current IoT environment in terms of device use and planned use by surveying a sample of Commonwealth agencies (see [Appendix](#)) where we believed IoT devices were used for significant purposes. Some of the important feedback from this survey included the following:

- Sixty-eight percent of respondents believe that the IoT has enabled their agencies to manage specific activities more efficiently. However, survey responses indicate that the adoption of IoT technology has been slow in the Commonwealth.
- Forty-three percent of respondents believe that the IoT is in its infancy and the risk of adopting IoT devices is greater than the benefits.
- Forty-six percent of respondents believe that IoT risks cannot be managed effectively and efficiently by current controls.

Our audit also assessed the adequacy of the internal controls that the Executive Office of Technology Services and Security (EOTSS)¹ has established for implementing and using IoT technology as well as the measures EOTSS has taken to mitigate security and privacy risks associated with the use of this technology. We found that controls in this area could be improved.

1. On August 1, 2017, the Governor established EOTSS to replace a previous agency, the Massachusetts Office of Information Technology, and made EOTSS responsible for administering the state’s information technology infrastructure.

According to EOTSS, the Massachusetts Access to Government Network (MAGNet)² will eventually be replaced by the One Network initiative, which will consolidate the specific agency networks into one centrally managed Commonwealth network. According to EOTSS, this will enhance network security and allow high network availability, fast network connectivity, centralized network monitoring, and centralized network traffic management.

Below is a summary of our findings and recommendations, with links to each page listed.

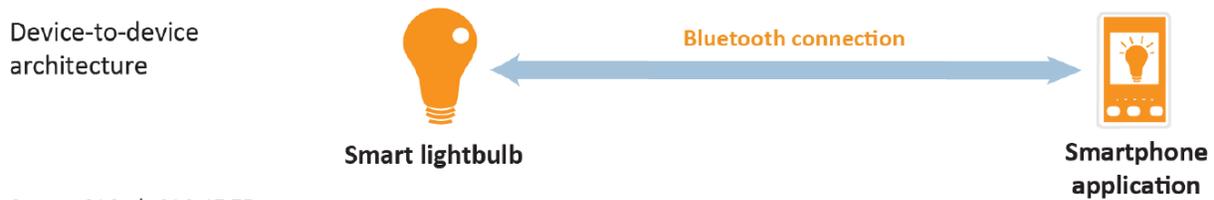
Finding 1a Page 11	The Commonwealth's Enterprise Information Security Policy (EISP) does not offer any guidelines to state agencies regarding the adoption of IoT technology.
Finding 1b Page 12	The Commonwealth does not have a formally documented information security incident response plan.
Finding 1c Page 13	The Division of Capital Asset Management and Maintenance did not involve the Commonwealth's chief information officer (CCIO) in a project that connected IoT devices to MAGNet.
Recommendations Page 14	<ol style="list-style-type: none">1. EOTSS should develop guidelines specifically for the IoT in its current EISP and incorporate them into its security policy. It could use the National Institute of Standards and Technology paper <i>NISTIR 8200—Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)</i> for reference.2. EOTSS should develop a documented information security incident response plan.3. EOTSS should implement a policy to ensure that all state agencies considering undertaking any projects related to MAGNet contact the CCIO and learn whether the CCIO should be involved in supervising the projects.

2. MAGNet is the Commonwealth's private geographically dispersed telecommunication network; it is managed by EOTSS and is used to connect the various local area networks used by state agencies.

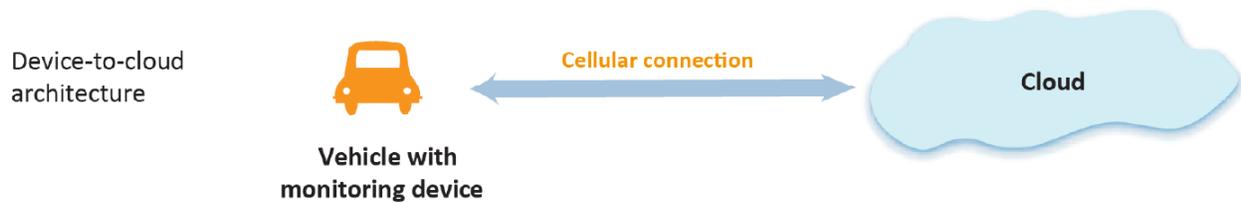
OVERVIEW

How Internet of Things Devices Communicate

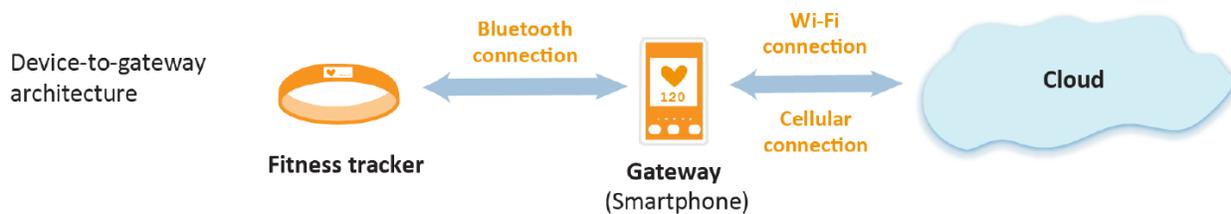
To operate and communicate data, Internet of Things (IoT) devices must be interconnected. The United States Government Accountability Office authored an assessment regarding the IoT in July 2017 titled *Internet of Things: Status and implications of an increasingly connected world* (GAO-17-75). This document provided a high-level understanding of the various ways IoT technology might be deployed from four basic architecture models: device to device, device to cloud, device to gateway, and cloud to cloud. The diagrams below, taken from GAO-17-75, depict the four models.



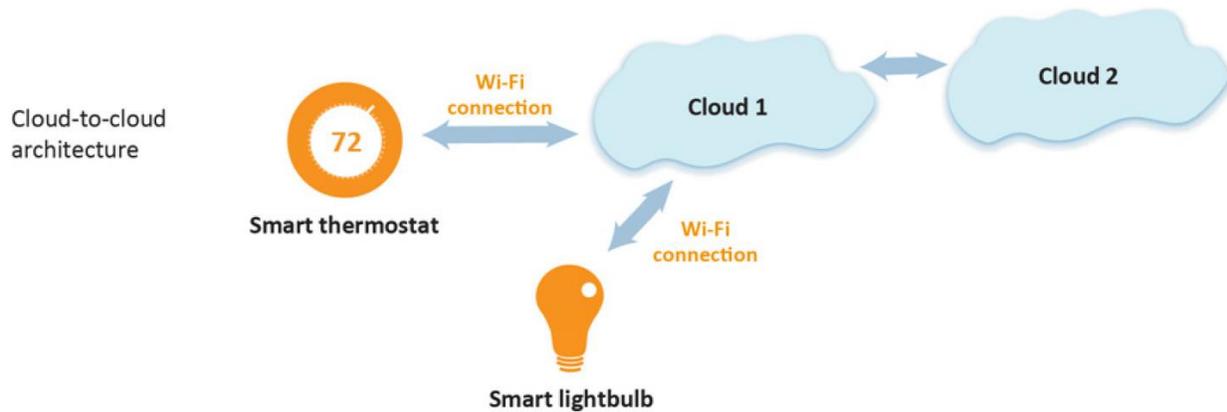
Source: GAO. | GAO-17-75



Source: GAO. | GAO-17-75



Source: GAO. | GAO-17-75



Source: GAO. | GAO-17-75

IoT in the Commonwealth

To obtain a better understanding of the current use of IoT devices by state agencies, the Office of the State Auditor conducted a survey of 84 state agencies, 28 of which responded. The purpose of this survey was to determine the current and future plans for deploying IoT devices in the Commonwealth, the types of IoT devices deployed, the ways information technology (IT) devices are connected to networks, the ways IoT devices are used, and agencies' perspectives on the benefits and risks of IoT technology.

For the purpose of our survey, we identified four types of IoT devices used, referred to as “waves” in this report. These waves are defined in a January 15, 2014 paper published by the SysAdmin, Audit, Network, Security (SANS) Institute, *Securing the “Internet of Things”*:

1. *PCs, servers, routers, switches and other such devices bought as IT devices by enterprise IT people, primarily using wired connectivity*
2. *Medical machinery, [supervisory control and data acquisition], process control, kiosks and similar technologies bought as appliances by enterprise operational technology (OT) people primarily using wired connectivity*
3. *Smartphones and tablets bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity*
4. *Single-purpose devices bought by both consumers, IT and OT people exclusively using wireless connectivity, generally a single form*

The most significant responses received from our survey include the following:

- All agencies were using general technology from the first wave of the IoT, and 24 out of 28 agencies were using third-wave devices such as smartphones and tablets. Five agencies indicated that they were using fourth-wave IoT devices, and 3 were using second-wave devices.
- Various agencies have different plans for using the IoT: 12 indicated that they planned to expand use, and 11 indicated that they did not have IoT plans currently but might in the future. Three agencies stated that they were not considering a plan for using the IoT.
- Nineteen out of 28 agencies believed that IoT consumer devices were available in the marketplace that could enable them to better manage a particular problem area. However, 8 of those 19 respondents also indicated that IoT devices that were relevant to the agencies were not yet available. Additionally, 5 agencies stated that they did not know if they were ready to adopt IoT devices.
- There were also differing opinions on adopting IoT technology. Twelve agencies agreed that IoT technology was in its infancy and the risk of adopting the use of IoT devices was greater than the benefits. Eleven agencies disagreed with these statements. Four agencies were unsure, and one did not answer.
- When asked about whether IoT technology risk could be effectively and efficiently managed by the current controls, 11 agencies said “yes,” 13 said “no,” 3 did not know, and 1 did not answer.
- Information that is collected at organizations includes data about energy and utilities, technology, consumer products and services, financial services and real estate, government, and healthcare and life sciences.
- There could be various effects at the agencies if IoT devices did not operate properly for a prolonged period, including program interruption (acknowledged by 12 agencies), financial effects (9 agencies), and public-safety issues (5 agencies).

There are no specific Massachusetts laws and/or regulations regarding the standardization of IoT use in the public sector. Rather, each Commonwealth agency is allowed to make its own business decisions in this area. Our survey results indicate that there is a lack of unity across the state. As previously discussed, the Executive Office of Technology Services and Security (EOTSS) is in the process of replacing the Massachusetts Access to Government Network with the One Network initiative, which will consolidate the specific agency networks into one centrally managed Commonwealth network. At the time of our audit, EOTSS was aware of the IoT; however, it did not provide any services to Commonwealth agencies regarding smart sensors or other IoT devices.

IoT Use by Commonwealth Agencies during the Audit Period

The Division of Capital Asset Management and Maintenance currently oversees the Commonwealth Building Energy Intelligence (CBEI) Program. The objective of this program is to measure energy use in state buildings and provide decision-makers with information that could be used to reduce energy use. The program includes participants from a significant number of state colleges and universities, state correctional facilities, state hospitals, trial courts, major state office buildings, water treatment facilities, power plants, and other sites. Currently, the IoT is used in smart building management³ within energy information systems to better understand when and how energy is used, identify cost-saving opportunities, and proactively maintain capital assets.

In the CBEI Program, agencies can use the collected data to monitor energy use from one period to the next and modify their building environmental systems to reduce energy use and carbon emissions, resulting in reduced costs as well as environmental benefits.

The next phase of the Commonwealth's smart building management initiative is to integrate the energy information system with an automated building control system at select sites to enhance energy savings performance. According to the US Department of Energy's Federal Energy Management Program, the United States federal government is one of the largest energy consumers in the world.

The Massachusetts Department of Transportation (MassDOT) Highway Division provides another example of IoT use. MassDOT has laid an infrastructure of fiber-optic cable underground to provide hardwired local area network connections to roadway surveillance cameras as well as motorist information signs placed along roads (depicted in the [Photos](#) section of this report).

In addition, cameras are used in electronic toll collection, which has eliminated tollbooths that hindered traffic flow. Drivers without transponder boxes have their license plate information gathered by IoT sensors and are billed based on the vehicle registration information. There are also electronic toll gantries on the Massachusetts Turnpike, which collect all-electronic tolling, take photos of license plates, and capture vehicle speeds. Photos of toll gantries are shown in the [Photos](#) section of this report.

IoT technology is also used by the Massachusetts Bay Transportation Authority (MBTA), the Department of Transitional Assistance (DTA), the Department of Public Health (DPH), and the Department of

3. Smart building management is the use of computer-based control systems to operate and monitor building functions and systems.

Environmental Protection (DEP). The MBTA uses global positioning system devices on trains to provide their locations and estimate their times of arrival at stations, which improves communication with riders.

DTA allows people to track their benefits with a phone application that lets them manage their cases, appointments, and contact information and check their balances.

DPH uses patient-monitoring systems in the intensive care unit at the Lemuel Shattuck Hospital to support decision-making and help improve patient care using a wired connection.

DEP uses sensors to collect data and measure air quality to track potentially harmful gases, particles, and toxins. DEP's MassAir Online website allows users to click on a state map to find real-time air quality data from DEP.

IoT Challenges

According to our interviews with IT professionals, the major IoT challenges facing the Commonwealth are cybersecurity, privacy, connectivity, and a lack of laws and regulations regarding the use of IoT technology. A cybersecurity attack such as a data breach or a denial-of-service attack⁴ can affect the social, political, and economic wellbeing of a particular person, organization, or government and, according to our survey, can be conducted for various reasons, such as financial gain, malicious intent, recognition, or revenge.

Every device that is connected to an organization's network increases the opportunities for it to be attacked by a hacker. According to a 2016 PricewaterhouseCoopers⁵ survey on information security breaches, the question is not whether a data breach will occur, but when. Anything that has an Internet Protocol address could be hacked. As the world becomes interconnected, cybercriminals have more opportunities to perform cyberattacks.

The IoT also poses challenges related to laws and regulations; for example, manufacturers are not required to implement a certain level of security in their IoT devices. This has caused devices to be susceptible to compromise by potential hackers.

4. According to the Information Systems Audit and Control Association's website, a denial-of-service attack is "an assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate."

5. PricewaterhouseCoopers is an international consulting, accounting, and auditing firm.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has completed a performance audit of the administration of the Internet of Things (IoT) at various Commonwealth agencies for the period July 1, 2016 through March 31, 2017.

We assessed the services that the Executive Office of Technology Services and Security (EOTSS) provided to agencies that were adopting the IoT. We also reviewed the Division of Capital Asset Management and Maintenance (DCAMM) Commonwealth Building Energy Intelligence (CBEI) Program because, as an IoT project, it uses devices with an Internet connection at various state hospitals, prisons, universities, community colleges, trial courts, and office buildings to measure energy use in state buildings and provide decision-makers with information that could be used to reduce energy use.

In conducting this audit, we reviewed key reports, attended conferences, conducted the aforementioned survey, and interviewed key state agency officials to obtain their views on the specific implications of the IoT.

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.

Below is our audit objective, indicating the question we intended our audit to answer and where the objective is discussed in the audit findings.

Objective	Conclusion
1. Is there adequate administration of IoT use at various state agencies?	No; see Findings 1a , 1b , and 1c

We conducted this audit using criteria from industry standards established by the National Institute of Standards and Technology. Although the Commonwealth is not required to follow these industry standards, we believe they represent information technology (IT) industry best practices. We formally engaged EOTSS to evaluate its roles and responsibilities related to providing cybersecurity and

governance to state agencies to manage current and emerging IT risks. OSA also engaged DCAMM to observe its implementation of IoT technology for smart building management in its CBEI Program.

This audit was intended to provide an understanding of the Commonwealth's administration of the IoT.

To achieve our objective, we performed the following audit procedures:

- We sent a survey to 84 agencies to gain an understanding of the current and future plans for deployment of IoT devices in the Commonwealth, the types of IoT devices deployed, the ways IoT devices are connected to networks, the purposes IoT devices serve, and agencies' perspectives on the benefits and risks of IoT technology. Twenty-eight of the agencies responded.
- We obtained an understanding of the implications of the state government adopting IoT technology through interviews with the chief information officer of the City of Boston and professors from the University of Massachusetts, Harvard University, and the Massachusetts Institute of Technology. In addition, we gained insight from chief information officers, chief information security officers, and IT management from EOTSS, DCAMM, the Massachusetts Department of Transportation, the Executive Office of Public Safety and Security, the Executive Office of Energy and Environmental Affairs, the Massachusetts Port Authority, the Department of Public Health, and the Executive Office of Health and Human Services.
- We reviewed reports, academic research, online webinars, and documents and attended conferences to gain a better understanding of the IoT.
- We reviewed DCAMM's IoT data security classification and determined whether the data were adequately protected when in transit and when stored.
- We reviewed the current and potential impact of the lack of governmental oversight over the adoption of IoT technology.

Further, at EOTSS, we performed the following work:

- We reviewed the applicable network security controls in the Massachusetts Access to Government Network that were intended to safeguard against potential security vulnerabilities of IoT devices and related information system resources.
- We reviewed the procurement and project management methodology for the CBEI Program and determined whether cybersecurity risks were properly mitigated.
- We reviewed asset management processes and verified the effectiveness of physical security for IoT devices and related IT resources.
- We reviewed the IoT vendor selection and vendor relationship management processes, as well as the availability of state data upon vendor termination.

- We reviewed the problem management and patch management⁶ processes for IoT devices and related IT resources.

The results of our survey of state agencies were not used to support our findings, conclusions, or recommendations; they were used for background and contextual information only. Therefore, a data-reliability assessment of the survey data was determined to be unnecessary.

We also assessed the reliability of DCAMM's IoT inventory list. Specifically, we reviewed existing information and interviewed knowledgeable staff members about the data. In addition, we performed validity and integrity tests on all data, including testing to determine whether (1) data were missing from relevant fields, (2) data were consistent with overall aggregate formatting, and (3) data were within the correct data range. We determined that the data provided to us by DCAMM were reliable.

6. According to the Information Systems Audit and Control Association's website, patch management is "an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk."

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Commonwealth needs to take additional measures to ensure the effective and efficient adoption of Internet of Things technology.

Although the Commonwealth has taken, and continues to take, measures to improve its information technology (IT) operations and security, we identified areas where IT administration could be improved to ensure the effective and efficient adoption of Internet of Things (IoT) technology. These areas include improving information security policies, standards, and guidelines; creating an information security incident response plan; and connecting IoT devices to the Commonwealth network with the involvement of the Commonwealth's chief information officer (CCIO) or his/her designee.

a. The Commonwealth's Enterprise Information Security Policy does not offer any guidelines to state agencies regarding the adoption of IoT technology.

The Commonwealth's Enterprise Information Security Policy (EISP) does not provide guidance to state agencies regarding the IoT. Specifically, it lacks controls to ensure that a minimum level of security is provided throughout the Commonwealth for the IoT, as well as optional control recommendations based on industry best practices, like those of the National Institute of Standards and Technology (NIST). Without adequate administration through policies, standards, and guidelines, the Commonwealth may be subject to security vulnerabilities that could affect its operations, safety, and privacy.

Authoritative Guidance

According to Section 4 of Executive Order 504,

The Commonwealth's Chief Information Officer . . . shall have the authority to:

- *issue detailed guidelines, standards, and policies governing agencies' development, implementation and maintenance of electronic security plans.*

Such guidelines, standards, and policies would support the Commonwealth's information security goals by protecting its information. To effect proper security over Commonwealth information, the CCIO should establish detailed policies, procedures, and standards regarding the connection, use, and security of IoT devices.

According to a NIST interagency paper, *NISTIR 8200—Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, the following are examples of gaps between existing cybersecurity standards and those that apply to the IoT:

Cyber Incident Management: *best practices for remediation when software patches are not feasible . . .*

Network Security: *existing standards may require updates and/or new standards will be needed to address IoT networks that have the potential for spontaneous connections . . .*

Security Automation & Continuous Monitoring: *since the IoT ecosystem is heterogeneous, IoT device manufacturers and security vendors may need to develop device-specific agents and interfaces for monitoring until the standards are tailored for the various IoT use cases and implemented in products . . .*

System Security Engineering: *need to determine if generic system security engineering standards . . . consider IoT systems.*

Reasons for Noncompliance

Management at the Executive Office of Technology Services and Security (EOTSS)⁷ acknowledged that the office's policies, procedures, and standards lacked specificity regarding the IoT. EOTSS stated that it was in the process of developing new policies, procedures, and standards. Despite the lack of specific IoT guidance, EOTSS stated that many of the security controls required to mitigate and counter IoT-based attacks were already fundamental to the existing network security, access controls, and other well-established security areas.

b. The Commonwealth does not have a formally documented information security incident response plan.

EOTSS has an Enterprise IT Security Incident Response Policy and Enterprise Security Incident Handling Procedures, but it does not have a documented incident response plan. Such a plan would establish specific procedures EOTSS would follow to respond to and resolve any detected incidents affecting the security of the Commonwealth's IT hardware, software, and data related to IoT devices. Without an incident response plan, the Commonwealth has inadequate assurance that it can effectively respond to and minimize the risk of cyberattacks when they happen.

7. EOTSS manages the Commonwealth's IT environment.

Authoritative Guidance

The NIST Incident Response Plan establishes the following best practices:

The organization:

- a. *Develops an incident response plan that:*
 1. *Provides the organization with a roadmap for implementing its incident response capability;*
 2. *Describes the structure and organization of the incident response capability.*

Reasons for Noncompliance

According to EOTSS management, the office has a draft incident response plan but has not yet published it.

c. The Division of Capital Asset Management and Maintenance did not involve the CCIO in a project that connected IoT devices to the Massachusetts Access to Government Network.

The Division of Capital Asset Management and Maintenance (DCAMM) procured the contract for a project that involved connecting IoT devices to the Massachusetts Access to Government Network (MAGNet) without involving the CCIO. Because the CCIO was not given the opportunity to participate in the project, there is inadequate assurance that the connected devices were properly connected, and there is an increased network security risk that IoT devices will be exposed to cyberattacks.

Authoritative Guidance

Section 11(a) of Executive Order 549 states,

The CCIO shall supervise all Executive Department IT project selection, development and maintenance, and shall supervise procurement in consultation with the Assistant Secretary for Operational Services.

Reasons for Noncompliance

DCAMM did not contact the CCIO to participate in this project because it classified the project as an energy group project, not an IT project. At the time of our audit, there were no controls in place that would allow the CCIO to monitor executive departments' compliance with the above requirement, nor are there policies and procedures that require executive agencies to consult with the CCIO on

any projects they are undertaking that may contain IT-related components to learn whether the CCIO should be involved in supervising the projects.

Recommendations

1. EOTSS should develop guidelines specifically for the IoT in its current EISP and incorporate them into its security policy. It could use *NISTIR 8200—Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* for reference.
2. EOTSS should develop a documented information security incident response plan.
3. EOTSS should implement a policy to ensure that all state agencies considering undertaking any projects related to MAGNet contact the CCIO and learn whether the CCIO should be involved in supervising the projects.

Auditee's Response

The responses to Findings 1a and 1b were provided by EOTSS. Regarding Finding 1a, the agency stated,

EOTSS was established by the Governor on August 1, 2017 replacing the agency commonly known as MassIT. The role of EOTSS was greatly expanded from what had been established for MassIT (or the Information Technology Division) through Executive Orders from previous administrations. These Executive Orders, specifically E.O. 504, gave MassIT limited oversight into IT security across the Commonwealth Executive Department but still allowed for significant fragmentation within IT and IT security.

Following its establishment as the central IT authority for the Executive Department, EOTSS created the first set of comprehensive Enterprise IT Policies and Standards, producing sixteen documents that cover core security principles. These documents will be reviewed annually; supporting documents, including Guidelines and Procedures, will be added as needed. EOTSS leveraged well-established security frameworks, mapping policies and guidelines to the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), the NIST Cybersecurity Framework (CSF), and the Center for Internet Security's "Critical Security Controls" ("the CIS Top 20").

EOTSS recognizes the growing impact of IoT and anticipates the need for additional guidelines. However, as the [Office of the State Auditor, or OSA] report explains, "the adoption of IoT technology has been slow in the Commonwealth." EOTSS believes that the focus must be on expanding and strengthening the underlying security infrastructure and operations that will be needed to support any such guidelines. Additionally, the growth of IoT has been challenging for many organizations, including those referenced in the [OSA] report. The NIST report cited by [OSA], Draft NISTIR 8200, was released in February of this year, was open for comments until April of this year, and remains a draft publication. This document includes no fewer than seven potential definitions of the term "Internet of Things." As NIST, CIS, and other high-quality security standards organizations clarify definitions and develop tested guidelines for this rapidly

expanding area of technology, EOTSS will ensure that the Commonwealth's policies and standards include appropriate security controls.

We note that the lack of the specific use of the term "Internet of Things" in our security policies does not indicate the absence of relevant security controls. . . . The majority of the recommendations in the draft NIST report are covered in other EOTSS policies, standards, guidelines and procedures including the following:

- *Encryption at rest and in transit*
- *Identity and Access Management*
- *Centralized security log aggregation (SIEM [Security Information and Event Management])*
- *Ongoing discovery and vulnerability scans*

While IoT devices represent a new threat vector that requires careful analysis, many of the security controls required to mitigate and counter IoT-based attacks are already fundamental to network security, access control, and other well-established security domains.

Regarding Finding 1b, EOTSS stated,

The Commonwealth Incident Response Plan, which unifies the disparate incident response plans developed under E.O. 504, has been in draft form since February and builds on the policies and procedures described above. We expect to publish this Incident Response Plan in the first quarter of Fiscal Year 2019, and we are happy to provide a copy of the draft document to [OSA]. We also note that the development and implementation of a unified Incident Response Plan for the Executive Department is dependent on a number of EOTSS' IT transformation initiatives, including the "One Network" project and significant upgrades to end user computing security.

The response to Finding 1c was provided by DCAMM:

DCAMM acknowledges that the CCIO was not directly involved in the procurement for the Commonwealth Building Energy [Intelligence] (CBEI) program. DCAMM would like it noted that internal IT staff was consulted early in the CBEI procurement. In addition to the fact that the CBEI program is aimed at energy consumption reduction, the team determined CBEI was not primarily an IT procurement for several reasons, including: each of the agencies involved in the CBEI program is responsible to manage its own MAGNet connections; the meters under the CBEI program were already installed and connected under a prior contract; and this stage of the CBEI program would only read utility data (which is already being reported by utility providers).

DCAMM and EOTSS have been in communication for the past 6 months concerning the CBEI program and other energy coordination opportunities. We will be implementing practices recommended in the course of this review, such as developing clear communication roles and responsibilities for any updates to enterprise security policies.

DCAMM would also like to clarify that in its current state the CBEI program is a monitoring program that does not include remote or automated building management. Though a future phase of this program involves reading Building Management System reports (this has not yet been deployed) there is currently a "read only" connection [that] does not control any building systems. The CBEI program provides participating agencies with real-time data on the energy consumption of its facilities. Each agency and facility is then responsible for adjusting building systems locally based upon the data and with recommendations from DCAMM. Should the CBEI program be expanded in the future to include building system controllability, DCAMM would coordinate with EOTSS and address network security concerns.

Auditor's Reply

As noted above, the policies that EOTSS administered during our audit period made no reference to the IoT. OSA acknowledges that EOTSS had mitigating controls in place that protected the Commonwealth's IT infrastructure. However, given the unique nature of connecting IoT devices to the Commonwealth's network, the continued expansion of the use of IoT devices by state agencies, and the potential threats involved with the management of these devices, OSA believes that the Commonwealth's EISP should provide specific guidance to state agencies regarding the IoT. For example, such guidance could include what controls are needed to ensure that a minimum level of security is provided throughout the Commonwealth for the IoT, as well as optional control recommendations based on industry best practices, such as those recommended in *NISTIR 8200*. Based on its response, EOTSS is taking measures to address our concerns in this area.

As stated above, during our audit period, EOTSS did have an Enterprise IT Security Incident Response Policy and Enterprise Security Incident Handling Procedures. However, in its response, EOTSS acknowledges that the Commonwealth Incident Response Plan has been in draft form since February. Based on its response, EOTSS is taking measures to publish the Commonwealth Incident Response Plan in the near future.

Based on its response, DCAMM is taking measures to address our concerns regarding working with EOTSS on its CBEI Program. OSA believes that in addition to this, EOTSS should implement a policy to ensure that all state agencies that consider undertaking any projects related to MAGNet contact the CCIO and learn whether the CCIO should be involved in supervising the projects.

APPENDIX

Agencies That Responded to Our Survey

Center for Health Information and Analysis
Commission for the Blind
Commission for the Deaf and Hard of Hearing
Department of Children and Families
Department of Developmental Services
Department of Fire Services
Department of Mental Health
Department of Public Health
Department of Transitional Assistance
Department of Veterans' Services
Department of Youth Services
Disabled Persons Protection Commission
Division of Banks
Division of Capital Asset Management and Maintenance
Division of Insurance
Executive Office of Elder Affairs
Executive Office of Health and Human Services
Executive Office of Technology Services and Security
Human Resources Division
Massachusetts District Attorneys Association
Massachusetts Office on Disability
Massachusetts Rehabilitation Commission
Municipal Police Training Committee
Norfolk District Attorney
Office for Refugees and Immigrants
Soldiers' Home in Chelsea
Soldiers' Home in Holyoke
Worcester County District Attorney

PHOTOS



Motorist information signs on a Massachusetts highway



Electronic toll gantry



Electronic toll gantry