



EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

CHARLES D. BAKER
Governor

Curtis M. Wood
Secretary

KARYN E. POLITO
Lieutenant Governor

February 15, 2021

Michael J. Heffernan
Secretary of Administration and Finance
State House, Room 373
Boston, MA 02133

The Honorable Suzanne Bump
State Auditor
State House, Room 230
Boston, MA 02133

Chair Aaron Michlewitz
House Committee on Ways and Means
State House, Room 243
Boston, MA 02133

Chair Michael Rodrigues
Senate Committee on Ways and Means
State House, Room 212
Boston, MA 02133

Dear Secretary Heffernan, Auditor Bump, Chair Michlewitz, and Chair Rodrigues:

Pursuant to Chapter 227 of the Acts of 2020, the Executive Office of Technology Services and Security (EOTSS) is pleased to provide you with the enclosed report detailing initiatives undertaken by EOTSS over the previous 12-month period to modernize the Commonwealth's information technology (IT) infrastructure and enhance its cybersecurity posture.

I am grateful for your continued partnership with EOTSS. Please feel free to contact Scott Ahern at scott.m.ahern@mass.gov should you have any questions about this report.

Sincerely,

Curtis M. Wood
Secretary, Executive Office of Technology Services and Security, and Chief Information Officer
of the Commonwealth of Massachusetts



Executive Office of Technology Services and Security

Annual Legislative Report

February 2021

Purpose of this Report

The Executive Office of Technology Services and Security's (EOTSS) 1790-0100 line item in the Fiscal Year 2021 operating budget includes language requiring EOTSS to report on various aspects of IT consolidation in the Commonwealth as well as the secretariat's operations and efficiencies:

"...that not later than February 15, 2021, the executive office shall file a report with the secretary of administration and finance, the state auditor and the house and senate committees on ways and means that shall include, but not be limited to, the following: (i) financial statements detailing savings and, where applicable, additional expenses realized from the consolidation of information technology services within each executive office and other initiatives; (ii) the number of personnel assigned to the information technology services within each executive office; (iii) efficiencies that have been achieved from the sharing of resources; (iv) the status of the centralization of the commonwealth's information technology staffing, infrastructure and network and cloud hosting; (v) the status of the commonwealth's cybersecurity; and (vi) strategies and initiatives to further improve the: (a) efficiency and security of the commonwealth's information technology; and (b) transparency of the executive office with the legislature, other executive branch agencies and the general public..."

EOTSS is heavily involved in what we like to call 'the future of work' for the Commonwealth. The COVID-19 pandemic has highlighted the importance of the Commonwealth's consistent investment in technology to support continuity of government and a more secure and resilient government. EOTSS has supported a remote and hybrid workforce of business and IT organizations throughout state government to maintain delivery of government services and will continue to apply innovative solutions to challenges facing the Commonwealth both related and unrelated to its COVID-19 response.

Savings, Efficiencies, and Additional Expenses through Consolidation

Under its Article 87 mandate, EOTSS is granted the authority to centralize IT personnel, programs, and policies at the enterprise level. The goal of consolidating strategically identified IT infrastructure and personnel is to eliminate redundancies, find efficiencies, and to standardize and enhance the Commonwealth's previously disparate cybersecurity and IT infrastructure at an enterprise level. Strategic centralization can also improve the efficiency and effectiveness of the services being consolidated.

Similarly, it is possible for cost savings to be achieved by leveraging economies of scale. Conversely, additional expenses can be incurred by the creation or expansion of IT services and security programs established to meet the growing demands of the digital era and increased cyber threats. Adopting new business models that have become the industry standard in the private sector, including the use of Software as a Service (SaaS) products, can be a vital solution in avoiding multimillion dollar capital expenditures on customized software builds and upgrades to legacy systems to support the applications they support.

Software and Contract Management Program

EOTSS established an enterprise-wide software licensing and contract management program. This program focuses on creating standardized procurement processes and asset management of software licensing for the Executive Branch. Centralized procurement and management of enterprise software licensing provides for more strategic acquisition and timely distribution of licenses. Moreover, centralized asset management and in-time deployment of software via subscription services results in improved accountability and cost avoidance against over-deployment charges that have negatively impacted the Commonwealth for years.

To date, through this approach, EOTSS has negotiated and established highly discounted enterprise volume licensing agreements with several major software providers, resulting in millions of dollars of annual savings for the Commonwealth (license costs, maintenance, and cost avoidance for over deployment), and more importantly a structured centrally managed program that ensures that our software deployments across the Commonwealth are up-to-date with the latest releases, including security patches and bug fixes. The cost avoidance gained in maintaining up-to-date software systems can be measured in operational impacts to government services resulting from security breaches or system failures due to unsupported or compromised software.

IT Investment Advisory Board

We are grateful to the Legislature for its commitment to investing in the Commonwealth's cybersecurity and IT modernization through the passage in 2020 of Governor Baker's General Governmental Bond Bill, which included \$650 million in IT capital authorizations. The IT Investment Advisory Board, comprised of security, IT, and business operations executives from across state government meets monthly to review IT capital project proposals. The Board helps ensure that this capital funding is allocated strategically on projects that align with the Commonwealth's goals of enhancing its security and improving its delivery of government services for the people of the Commonwealth.

COVID-19 Response

Within weeks of Governor Baker's State of Emergency Declaration, over 20,000 Commonwealth employees were working remotely. To avoid a duplicative effort from across the Executive Branch, EOTSS leveraged an enterprise approach in procuring 7,200 new devices to support the rapid shift to a remote workforce. With a dramatic increase in employees remotely connecting into Commonwealth systems, EOTSS deployed a new virtual private network (VPN) to increase bandwidth and capacity to support the remote workforce. The deployment of the new Commonwealth owned and managed VPN environment, in tandem with the retirement of a legacy vendor-owned VPN environment offers the Commonwealth more capacity for concurrent users, autonomy, and cost savings.

Additionally, EOTSS expedited the enablement of the Microsoft Office 365 license to end users at the request of secretariat chief information officers (SCIOs) across the Executive Branch to allow for immediate access to remote collaboration tools like Teams, OneDrive, and Sharepoint. EOTSS also enrolled thousands of employees in multi-factor authentication (MFA) and identity access management services to enhance the Commonwealth's cybersecurity framework.

Cloud Computing

Strategically migrating Commonwealth systems to the cloud can also serve as another cost avoidance measure. Cloud services offer high availability, resiliency, and scalability for Commonwealth systems – resulting in improved business application performance and improved user experiences.

With the adoption and usage of cloud computing subscription services a net increase in operating expenses must be accounted for; however, unplanned or emergency replacements or upgrades to Commonwealth systems that are budgetarily unaccounted for are mitigated. Unplanned or last-minute system upgrades are more expensive and present a greater risk. They often result in business interruptions that may have significant negative impacts to our constituents.

We have also adopted a multi-cloud strategy to promote competition between cloud service providers. Additionally, EOTSS takes advantage of discount programs offered by its cloud providers, including prepayment and preplanned spending plans. Another savings for the Commonwealth is the elimination of oversized and often under-utilized hardware and software platforms that have been the norm rather than the exception in our state data centers. Immediate benefits to moving to the cloud include greater availability, scalability and resiliency of the business applications and systems that are hosted.

Investment in cloud transition is significant and is being funded through our capital bond program. EOTSS continues to work with state agencies and Administration and Finance to build out the annualized costs for steady state operations.

Executive Branch IT Personnel

From retail banking shifting to mobile banking or the rise in telehealth services, industries across the economy are evolving to meet the demands of the digital era. As businesses evolve, our constituents expect more and more from their government. It is critical that as a Commonwealth, we continue to innovate and invest to improve our delivery of government services to meet this increasing demand. We are living in a digital era – constituents are interacting with government services increasingly in a digital format rather than face-to-face interactions in a brick-and-mortar setting. As such, we can expect an increased need for additional skilled personnel in certain IT roles to develop, implement, and support these digital services.

EOTSS continues to seek out strategic opportunities to centralize IT staffing personnel where an enterprise focus can increase the efficiency or effectiveness of the Commonwealth's cybersecurity posture and IT service delivery. Often times, maintaining IT personnel at each secretariat across the Executive Branch ensures that the IT staff most directly connected with and knowledgeable of their specific business applications are directly involved with IT business transformations. This structure allows EOTSS to focus on security and technology infrastructure at the enterprise level, while IT personnel in the secretariats can more closely focus on business applications and service delivery to the constituents they serve.

The following chart shows the number of IT personnel who support IT infrastructure and business applications within each executive office as of February 2021:

Secretariat	Number of IT Personnel
A&F	189
EOE	38
EEA	51
HHS	492
HED	25
LWD	45
EPS	23
TSS	370
DOT	38
<i>TOTAL</i>	<i>1271</i>

Status of Centralization of Infrastructure, Network, and Cloud Hosting

For many years now, the Commonwealth has recognized the importance of supporting investments in modernizing its IT infrastructure, formalizing this support with the establishment of EOTSS as the Commonwealth's lead IT organization in 2017. This leadership laid the foundation for a more adaptable and flexible approach to IT services within the Commonwealth. These investments were critical in the Commonwealth's ability to maintain continuity of government services in the wake of the COVID-19 pandemic. In conversations with our peers in other states, it is clear that the Commonwealth's focus on innovation allowed us to be more resilient in our ability to maintain the delivery of government services to the most vulnerable populations at a time when government services were so greatly needed.

COVID-19 Response

As mentioned above, EOTSS deployed a new VPN environment within weeks of the Governor's State of Emergency Declaration to increase bandwidth and capacity to support the rapid shift to a remote workforce. The ability to stand this new environment up so quickly was due to investments made by the Legislature and planning and preparation made by EOTSS to modernize the Commonwealth's IT infrastructure.

Likewise, EOTSS' procurement of 7,200 new devices to support a rapid shift to a remote workforce was made possible in part by groundwork laid in advance of the outbreak of the pandemic. In an effort to procure uniform devices for all Commonwealth employees, EOTSS has undertaken its Modern Workplace Initiative. Leveraging economies of scale, this initiative will ultimately ensure that all

Commonwealth employees are using uniform devices capable of supporting a suite of productivity and collaboration tools to for our workforce to work effectively and securely.

The outbreak of the pandemic resulted in unprecedented claims volume for unemployment insurance (UI). While many legacy state UI systems broke due to their brittleness and lack of agility, the Commonwealth was able avoid these issues by EOTSS and the Labor and Workforce Development (LWD) secretariat standing up cloud contact centers for the Department of Unemployment Assistance (DUA). Leveraging our experience and partnerships in cloud computing and services, a cloud solution for this massive spike in claims volume offered flexibility and rapid scalability that a legacy on premise system would be unable to provide, ensuring constituents in need of UI and Pandemic Unemployment Assistance (PUA) received their checks in a timely fashion.

Infrastructure, Network, and Cloud

EOTSS has completed the design of its new One Network Core. This represents the consolidation from disparate networks into a single Commonwealth core. In this, we have eliminated unnecessary legacy agency network cores and overlapping internet protocol (IP) space to simplify the routing of data that occurs between networks. Security measures have been put into place to block off any 'back doors' by removing the many different internet connections previously located at each Executive Branch secretariat, enhancing the Commonwealth's security, providing higher availability and resiliency, and saving money by tapping into commodity services instead of requiring custom buildouts.

Moving forward, EOTSS will make further enhancements to the Commonwealth One Network by building out the wide area network (WAN) and security services to account for and support increased resiliency, mobility, and remote management.

Migrating Commonwealth systems from on premise data centers to a cloud solution is a smart decision. Cloud services provides the Commonwealth best-in-class technology that allows for incremental improvements in a faster, agile manner. They also provide the ability to react to increased demands, reduce time to provision and deprovision licenses, and more efficiently manage assets. More importantly for today's work environment, cloud services strengthen security services to support remote access to our systems from any location, further enabling the Commonwealth's remote workforce.

EOTSS works closely with the Secretariat Chief Information Officers (SCIOs) and business application owners at Executive Branch secretariats to best understand their business needs and prepare for the 'lift and shift' of Commonwealth systems to the cloud to ensure continuity of those government services. Over the past year, EOTSS has led the migration of 11 additional Commonwealth systems to the cloud, (including the state payroll system HR/CMS) and currently have 31 additional projects in the queue. Since 2017, EOTSS has coordinated the migration of over 300 Commonwealth applications/platforms to the cloud services model. We continue to work with our agency partners to identify and prioritize opportunities for further cloud migrations.

As our focus remains on the 'future of work' for the Commonwealth, EOTSS has introduced the enterprise consolidated print services model, a software driven solution that provides for a centrally managed secure service for on premise and remote printing. This program also eliminates thousands of individual desk printers in lieu of high volume multi-functional devices staged strategically throughout

agencies, reducing costs to operate including reducing consumables such as toner and service calls for maintenance and repairs.

EOTSS has also recently procured and deployed Adobe E-Sign, an electronic signature tool that will further support digitization of paperwork and records.

Cybersecurity

Prior to EOTSS' establishment as a cabinet secretariat, the Commonwealth's cybersecurity apparatus was a patchwork of infrastructure, personnel, and policies decentralized across the Executive Branch. In the past few years, the Commonwealth has made immense progress in enhancing its cyber defenses. EOTSS has been following industry best practices and continues to seek out best-in-class solutions for securing the Commonwealth's data and systems. In an effort to stay up on the latest cybersecurity information, EOTSS maintains an ongoing dialogue with our partners and peers at (1) the national level – the Department of Homeland Security (DHS), the Cybersecurity Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Governor's Association (NGA), and the National Association of State Chief Information Officers (NASCIO) and 2) the state and local level – the Mass Cyber Center, the Advanced Cyber Security Center (ACSC), the Legislature and municipalities.

In its first years as a cabinet secretariat, EOTSS has focused on low-input, high-impact opportunities to improve the Commonwealth's cybersecurity posture, shoring up at-risk vulnerabilities in the Commonwealth's previously patchwork security system. The Commonwealth now has a set of standard cybersecurity practices in place where we can identify, mitigate, and remediate cyber threats. EOTSS has several initiatives underway to mature the Commonwealth's cybersecurity infrastructure to a 'steady state' where the focus will remain on readiness and preparedness. With continued support from the Legislature and execution by EOTSS and its partners, we are confident that we are taking the right approach and are on the path to a more resilient and secure Commonwealth.

Security Infrastructure

EOTSS continues to build out the capacity and services of its Security Operations Center (SOC) and its Security Incident Event Management (SIEM) system. The SOC routinely participates in a number of training exercises with industry partners to improve the Commonwealth's readiness and preparedness. Table simulation exercises provide the opportunity to improve our technical, legal, and communications response to cyber threats and simulated attack exercises inside a virtual environment allow our security professionals to follow the blueprint of the Commonwealth's security framework to train in identifying, mitigating, and remediating compromised systems.

The Commonwealth's SIEM system provides capacity and capability to provide enhanced security analytics of the Commonwealth's networks and information systems. With this platform, our security organization can detect, investigate, communicate, and mitigate cyber threats to our systems and data.

EOTSS' vulnerability management program is another critical component to the Commonwealth's security framework and approach. This program offers better visibility across the enterprise to identify vulnerabilities and work with Executive Branch secretariats to mitigate identified vulnerabilities. While

continued progress has been made through this program by prioritizing and addressing critical vulnerabilities of Commonwealth systems, EOTSS and state agencies must maintain vigilance and commitment to staying aware of persistent threats and operating a continuous and adaptive vulnerability management program to mitigate these ever-present threats.

Commonwealth and Municipal Cybersecurity Awareness Training

The Commonwealth provides cybersecurity end-user awareness training to all Commonwealth executive branch employees so they can be educated on how to remain vigilant and avoid falling prey to potential cyberthreats. By training our workforce, we essentially expand the number of the Commonwealth's cybersecurity team from a couple dozen to tens of thousands of employees. EOTSS supplements its cybersecurity training with enterprise phishing simulation exercises to gain a better understanding of the Commonwealth's endpoint vulnerabilities and to enhance its training materials.

In addition to the Commonwealth's workforce, EOTSS supports opportunities to assist our partners in municipal government. In 2019, EOTSS announced the first-ever Municipal Cybersecurity Awareness Grants, with over 42,000 municipal and public-school employees throughout the Commonwealth accessing training to better detect and avoid cyberthreats. In 2021, EOTSS will facilitate a new round of Municipal Cybersecurity Awareness Grants to provide this critical training to more of the Commonwealth's municipal and public-school employees.

Enterprise Risk Management Program

To improve transparency for business operations and minimize financial waste, EOTSS' Office of Enterprise Risk Management and the Security Team are developing an enterprise risk management program. Third-party risk is one of the biggest cybersecurity threats facing governments. Through a qualitative and quantitative assessment process, the enterprise risk management program will allow the Office of Enterprise Risk Management to scrutinize the maturity of the security and privacy standards that current third-party vendors and any apparent successful bidders have in place.

To lead the efforts of the enterprise risk management program, the Secretary appointed the Commonwealth's first Chief Risk Officer (CRO). The CRO has the primary role of supporting organizational governance and leadership with strategic and operational risk management for value creation and protection to ensure the Commonwealth's vendors are maintaining security standards on par or in excess to those of the Commonwealth.

Transparency with the Legislature, Executive Branch Agencies and the General Public

Oversight and Reporting on IT Spending

In coordination with our partners in the Legislature, EOTSS has developed and implemented systems for additional oversight and reporting for IT projects and procurement. For enhanced cost oversight and control, any IT project or procurement with expenses over \$200,000 made by an executive office or one of its' respective state agencies must be reported to and approved by the Chief Information Officer of the Commonwealth.

Additionally, on an annual basis, EOTSS provides a report to the State Auditor and Legislature detailing the complete accounting and justification for all IT expenditures over \$250,000. We appreciate the opportunity to share this information with the Legislature for increased transparency detailing how allocated funds are being invested in the Commonwealth's IT and cybersecurity infrastructure.

These reporting requirements support the mission of EOTSS and its IT Investment Advisory Board to ensure that taxpayer money is being invested wisely to improve delivery of government services and secure the Commonwealth's IT and data assets.

Mass.gov and AlertsMA

As a tool in the Commonwealth's COVID-19 response communications strategy, the EOTSS Interoperability Communications Bureau (ICB) engaged the Massachusetts-based company Everbridge, to launch AlertsMA, an emergency notification system designed to send important text, voice and email alerts directly to subscribers' devices. With the ability to send critical updates in more than ten languages to over 400,000 subscribers to the resident portal and keyword text campaigns, AlertsMA has proven to be a useful tool in the Commonwealth's public health response. EOTSS is also in the process of completing the rollout of this service to alert Commonwealth employees and contractors of important workplace updates related to weather and other emergencies.

e-discovery

The EOTSS e-discovery Team supports secretariats and agencies in the Executive Branch by providing technical tools and services for searching electronically stored email data located in multiple Commonwealth email systems and files. Legal departments across the Executive Branch are increasingly relying on digital tools to perform their work. To meet this increasing demand, the EOTSS e-discovery Team is actively engaged in the implementation of enterprise software capable of ingesting large volumes of electronic data from multiple sources beyond email data, such as desktop applications and network share drives.

This enterprise software solution offers Commonwealth lawyers the capability of using cutting-edge search, analysis, and visualization tools. The Commonwealth's investment in this type of robust enterprise software is expected to increase transparency and operational efficiencies in responding to legal requests, including public records requests (PRRs) and litigation.

Looking Forward

In closing, we at EOTSS thank the Legislature for the opportunity to showcase some of the work undertaken and underway at the enterprise level in collaboration with our IT and business partners from across state government. We welcome the continued partnership with the Legislature to find innovative solutions to tackle the challenges of the 21st century and to best position the Commonwealth to provide secure, first-class government services to the constituents we all serve.