Commonwealth of Massachusetts
Enterprise IT Strategic Plan: FY23 – FY25

Table of Contents

Overview

Technology remains critical to ensuring the availability of government operations and the efficient delivery of services to Massachusetts' many residents, businesses, and visitors. It is a key enabler for optimizing business processes, protecting constituent data, and improving the overall digital government experience.

As the Commonwealth's lead organization on Information Technology (IT) and Cybersecurity, the Executive Office of Technology Services and Security (EOTSS) is responsible for establishing a framework for the strategic planning, management, and delivery of IT and security systems and services for all Executive Branch agencies.

Per M.G.L. c. 7D, § 9, EOTSS has developed the following **Enterprise IT Strategic Plan for Fiscal Years 2023 – 2025** to help secretariat and agency leadership make informed decisions for their agencies and the impacts to their constituents.

The Enterprise IT Strategic Plan does not replace individual agency strategic plans, their respective IT strategic planning requirements under M.G.L. c. 7D, § 6, or the annual IT Capital Investment Plan, rather it helps agencies make technology decisions and investments that align with the Commonwealth's enterprise technology efforts. Agency business and IT leadership are expected to be knowledgeable of this plan, to align their individual IT plans with the EOTSS-established framework and Standard Operating Environment (SOE), and to be compliant with all related enterprise policies, standards, and guidelines.

Together, the Secretariat IT Strategic Plans and this Enterprise IT Strategic Plan continue the march of the past two years towards a Commonwealth where all public services are accessible, reliable, and available wherever and whenever needed.

While non-Executive branch agencies are not required to adhere to the EOTSS framework, compliance and participation is *strongly recommended*.

A Message from the EOTSS Secretary and Chief Information Officer for the Commonwealth

The Baker-Polito Administration made the important decision five years ago to modernize our state-owned information technology (IT) systems and services, strengthen the Commonwealth's cybersecurity posture, and improve the constituent digital-government experience through the creation of EOTSS.

Since then, the Commonwealth has undergone transformational change by means of critical investments in core personnel, processes, and technologies to:

- Drive a new enterprise approach to IT infrastructure and services;

- Unify security operations, risk management, and data privacy frameworks;

- Ensure the continuity of government operations through a more resilient Commonwealth;

- Foster innovative technology solutions to enhance citizen-centric digital services; and

- Deploy a Standard Operating Environment (SOE) across all Executive Branch agencies.

COVID-19 highlighted the need for secure, available, mobile, reliable, and resilient technology systems and services to maintain the continuity of government operations and constituent services under the most difficult circumstances. The Commonwealth's increased focus in recent years on prioritizing resiliency by adopting cloud-based solutions, enabling a more flexible and mobile workforce, and expanding our digital services footprint enabled a strong and timely response to many of the unique challenges imposed by the pandemic.

Today, we find ourselves at a transformational moment as technology has become ever-more integrated into the way agencies conduct business and is relied upon more heavily for the continuity of government services. The COVID-19 pandemic response and subsequential shift toward a more mobile workforce and hybrid work environment accelerated business process redesign and the movement towards digital-centric services at an unprecedented pace.

Moving forward, the Commonwealth is looking to leverage the current interest and acceleration towards digital-centric services and a more resilient state government. Along with new opportunities for enhancing the citizen user experience and streamline agency business operations, there are opportunities in FY23-FY25 to expedite core investments in consolidated network infrastructure, complete the migration of applications and systems out of state-run data centers, and expand our unified Security Operations Center (SOC) capabilities and capacity.

As we close out FY22 and build an IT roadmap for FY23 and beyond, EOTSS will continue to promote and execute on its unique mission and strategies outlined above – while also focusing on the following areas of priority:

1. Cybersecurity and Enterprise Risk Management
2. Constituent/Customer Engagement Experience
3. Digital Services/Processes
4. Modernization of Legacy Applications, Systems, and Technologies
5. Cloud Computing – Public/Private Cloud Solutions

6. Infrastructure Modernization – Co-location/Infrastructure-as-a-Service (IaaS)
7. Sustainability Initiatives
8. Hire/Retain/Nurture IT Personnel
9. IT Governance
10. Introduction of Emerging Technologies

I encourage you to take some time to review and familiarize yourself with the Enterprise IT Strategic Plan for FY23 – FY25. This plan sets the direction, but it is up to us all to continue to work together to ensure that enterprise technology and digital investments are appropriately planned for and in line with business and technology strategic drivers.

Pro-active collaboration, communication, and engagement have helped us achieve our success to date. We must take the same approach as we set the course for the next phase of technology and security transformation in the Commonwealth.

I look forward to the road ahead!

Curtis M. Wood

Secretary/Commonwealth CIO

EOTSS Guiding Principles

EOTSS works in an integrated and collaborative approach with secretariat and agency partners to promote the Guiding Principles outlined below.

These Guiding Principles reflect the Administration's priorities of ensuring the continuity of government services, improving the citizen-centric digital experience, strengthening our cybersecurity posture, and modernizing our legacy technology infrastructure. Together, they help move the Commonwealth toward its collective IT and cybersecurity goals.

A Holistic Planning Approach

EOTSS has organized a holistic, enterprise approach to IT strategic planning for all secretariats. It evolves from an organization's mission and vision to the specific goals they hope to achieve over a 24-month time horizon. Secretariats then identify the strategies and initiatives they will deploy to reach their specified goals.

This approach synchronizes secretariat IT strategic planning with the annual IT Capital Planning process as well as the completion of this Enterprise IT Strategic Plan.

The EOTSS "Top 10"

All secretariat and agency strategic plans, programs, projects, and initiatives must take into consideration the following "Top 10" priorities from the EOTSS statewide IT strategy:

1. **Continuity of Government Services:** Ensure that solutions fit within the Modern Workplace framework and consider disaster recovery and the continuity of operations.

2. **Business Resiliency:** Applications and systems should move to approved cloud and modern third-party hosting solutions equipped to handle unexpected events and still perform at scale.

3. **Scalability:** Applications and systems should move to approved cloud and modern third-party hosting solutions that can scale up capacity to meet processing demands.

4. **Security:** All solutions and infrastructure should provide for end-to-end security with priority focus on cybersecurity and risk management.

5. **Mobility:** Ensuring workforce mobility through the Modern Workplace Program, associated collaborative toolsets, mobile device management solutions, and mobile application management solutions.

6. **Accessibility:** The ability to make information available to all authorized systems and users at any time and in any place in a secure, timely, and efficient manner.

7. **Availability:** All infrastructure should be fault tolerant, with the ability to switch over to alternate systems as needed.

8. **Flexibility:** Agencies should maintain the ability to add new services and/or functionality to a system without requiring a significant effort.

9. **Transparency:** Provide clear, simple, and well-defined interfaces, APIs and/or services to enable system and user interactions.

10. **Citizen-Centric Government:** Citizen-centric government is focused on user-centric design. Agencies must consider the full citizen user experience and tailor solutions to how real users interact with government services.

EOTSS Top Ten Priorities

1 **Continuity of Government Services:**
Ensure that solutions fit within the Modern Workplace framework and consider disaster recovery and the continuity of operations.

2 **Business Resiliency:**
Applications and systems should move to approved cloud and modern third-party hosting solutions equipped to handle unexpected events and still perform at scale.

3 **Scalability:**
Applications and systems should move to approved cloud and modern third-party hosting solutions that can scale up capacity to meet processing demands.

4 **Security:**
All solutions and infrastructure should provide for end-to-end security with priority focus on cybersecurity and risk management.

5 **Mobility:**
Ensuring workforce mobility through the Modern Workplace Program, associated collaborative toolsets, mobile device management solutions, and mobile application management solutions.

6 **Accessibility:**
The ability to make information available to all authorized systems and users at any time and in any place in a secure, timely, and efficient manner.

7 **Availability:**
All infrastructure should be fault tolerant, with the ability to switch over to alternate systems as needed.

8 **Flexibility:**
Agencies should maintain the ability to add new services and/or functionality to a system without requiring a significant effort.

9 **Transparency:**
Provide clear, simple, and well-defined interfaces, APIs and/or services to enable system and user interactions.

10 **Citizen-Centric Government:**
Citizen-centric government is focused on user-centric design. Agencies must consider the full citizen user experience and tailor solutions to how real users interact with government services.

Enterprise Objectives & Standard Operating Environment (SOE) Architecture

All secretariats and agencies must also account for the following EOTSS enterprise programs, projects, and initiatives as part of their strategic planning:

- **The Modern Workplace Program (MWP) Standard End User Set up**: A laptop (equipped with Windows 10 and Office Pro Plus with OneDrive, SharePoint, and Teams), monitor, docking station, keyboard, and mouse.

- **MWP Projects and Workstreams:** Such as personal and group file Migrations to SharePoint and OneDrive, email migrations.

- **Consolidation of the Active Directory into Azure AD**

- **One Network Consolidation**: Redesign and build of CORE Network and Wide Area Network (WAN) Optimization.

- **Enterprise Voice Solutions:** Migration to the MassVoice secure, private-cloud Unified Communications service tailored exclusively to MA state and local government clients.

- **Enterprise Cybersecurity Framework, Operations, and Incident Response and Reporting**

- **One Service Desk:** Moving toward One End-User Organization.

- **Infrastructure Hosting Solutions:** Strategies for moving out of state-run data centers and modernizing legacy IT infrastructure (Hybrid Cloud, On-premises -3rd-Party Hosting, IaaS, PaaS, and SaaS).

- **Application Rationalization:** Prioritization for modernizing, replacing, or upgrading key business applications and readying for migration to approved hosting solutions.

- **Enterprise Print Services:** Moving to a vendor-agnostic enterprise managed-print solution for multi-function devices located in agency offices and facilities.

The Road Ahead

Along with the IT Capital Investment Principles, the EOTSS Top 10 and the Enterprise Objectives provide agencies with a framework to ensure the continued availability of government operations and the efficient delivery of services to the residents, businesses, and visitors of the Commonwealth.

Moreover, the EOTSS Guiding Principles and holistic planning approach will help agencies to promote technology solutions that enable for optimizing business processes, protecting constituent data, and improving the overall digital government experience.

The goal is to continue working towards a Commonwealth where all public services are accessible, reliable, and available wherever and whenever needed.

Modern Workplace Program

In fall of 2019, EOTSS launched the Modern Workplace Program (MWP) – a carefully choreographed deployment of hardware, software and tools that promote data security, collaboration, and mobility. This initiative was the cornerstone of the overarching Commonwealth Workforce Mobility Program included in the Administration's FY21-22 Capital Plan to build a sustainable technology foundation ensuring a resilient, accessible, and scalable platform for the continuity of government services.

MWP by the Numbers
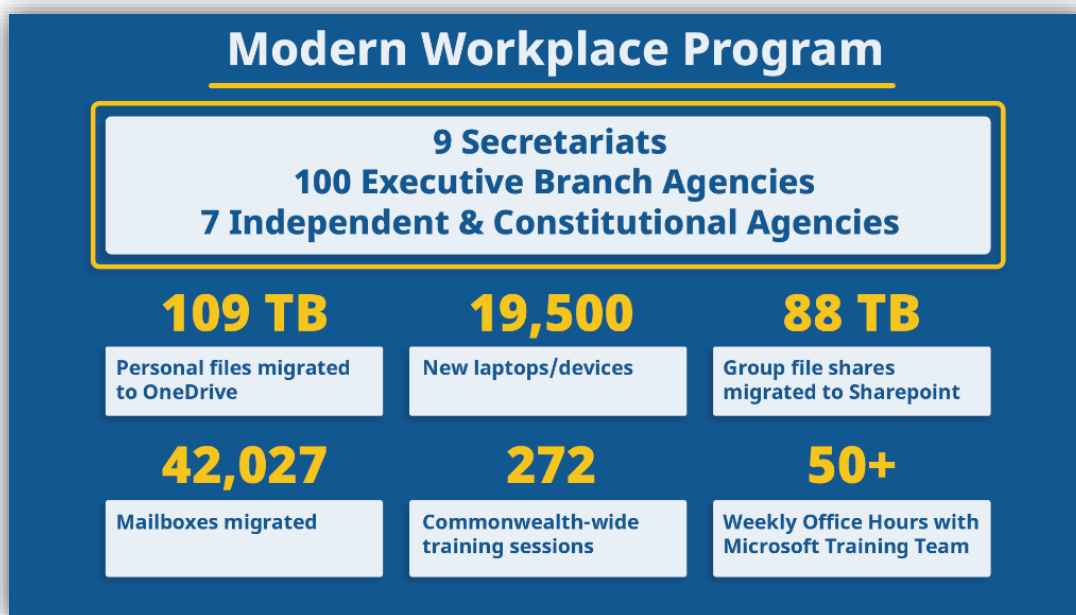
MWP Impact

Through the program workstreams, the Commonwealth addressed several inconsistencies, inequities, and security concerns in end-user hardware, software, and collaboration tools across the enterprise. More specifically, the MWP:

- Deployed a standard end-user hardware and software set up for all Executive Branch Employees (Windows 10 with O365 Pro Plus)

- Migrated personal employee files to the accessible and secure cloud-based solution OneDrive for Business – allowing access from anywhere on any device

- Moved group shared files to accessible and secure cloud-based SharePoint solution so that employees can access and collaborate on documents from anywhere on any device

- Migrated email off premise to more secure, resilient, and accessible Office 365 cloud solution

- Standardized on Teams as the enterprise standard for office collaboration and videoconferencing

Current	Future
Office Suite (On Premise) — Word, Excel, PowerPoint, Access	Excel: A familiar spreadsheet tool with new ways to view data and share insights Word: Collaborate on documents through state-of-the-art editing and sharing Powerpoint: Create shared presentations with real-time changes OneNote: Organize your notes and share with others Access: A relational database program that helps store information for reference, reporting, and analysis Publisher: A desktop publishing application to create graphic intensive documents
Local Drive	OneDrive for Business: A place to store and share your private documents, easily accessible from any device
Outlook	Everywhere access to email, contacts, and all-in-one calendar management
Skype, Slack, WebEx	Microsoft Teams: Collaborate with instant messaging, video conferencing, and live editing all while within one single application
SharePoint	SharePoint: Browser-based collaboration and document management
Windows 7	Windows 10: Modern operating system meant for an adaptive workspace and collaborative platform

Today, the MWP is enabling government to operate effectively under any circumstances after providing a springboard for the rapid acceleration of telework at the onset of the COVID-19 emergency.

Modern Workplace Program: FY23-25

Most of the program workstreams will be completed in calendar year 2022, fulfilling the Commonwealth's "Future of Work" needs by enabling a 21st century state workforce that is nimbler, consumes a smaller office footprint, and has access to updated hardware, software and productivity tools across all agencies.

However, EOTSS does anticipate a small number of new device deployments to continue into the first half of FY23 due to lingering global supply chain issues for technology equipment. Additionally, some personal and group shared file migrations for the larger secretariats will also continue into the fall due to the sheer volume of data that remains to be migrated.

Modern Workplace Program Priorities:

1. **Complete Remaining Workstreams:** Complete the small number of remaining device deployments and file migrations.

2. **Optimize O365 and Azure:** Ensure the Commonwealth is fully leveraging the capabilities of the cloud-based Microsoft Office 365 suite and the Azure Active Directory (AD) framework to support the strategic and tactical goals of promoting government business continuity and technical resiliency.

Cybersecurity & Enterprise Risk Management

Since its creation and elevation to the cabinet level secretariat in 2017, EOTSS has served as the enterprise IT organization and has taken the lead role in cybersecurity policy and strategy for the Executive Branch.

Key investments have been made to ensure the confidentiality, integrity, and availability of Commonwealth data, applications, and infrastructure. These investments include the development of an enterprise-wide security and risk management strategy, recruitment and engagement of skilled and experienced talent, procuring best-in-class technologies, and building a modern organizational structure to support operations.

Security Collaborations & Partnerships

The Commonwealth has also developed and maintained relationships and 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.
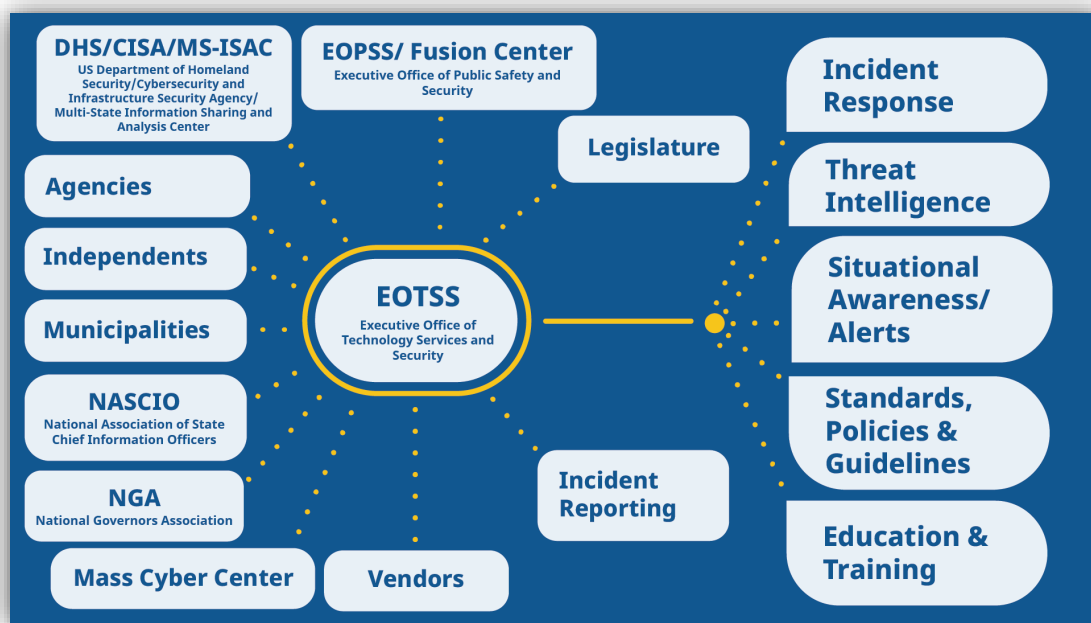
EOTSS and secretariat IT organizations routinely participate in training exercises with our federal, state, and industry partners to improve the Commonwealth's readiness and preparedness. Table simulation exercises provide the opportunity to improve our technical, legal, and communications response to cyber threats. 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.

Cyber Disruption Team

In late 2021, the Commonwealth's Cyber Disruption Team (CDT) was operationalized to respond to cyber threats and incidents across the state. This cross jurisdictional team, led by the Secretary of EOTSS is comprised of members that include the Commonwealth's Homeland Security Advisor, the Commonwealth Fusion Center, the Massachusetts State Police, Massachusetts National Guard, and the Massachusetts Emergency Management Agency, and is focused on providing additional subject matter expertise and capacity in preventing and responding to cyber threats and incidents.
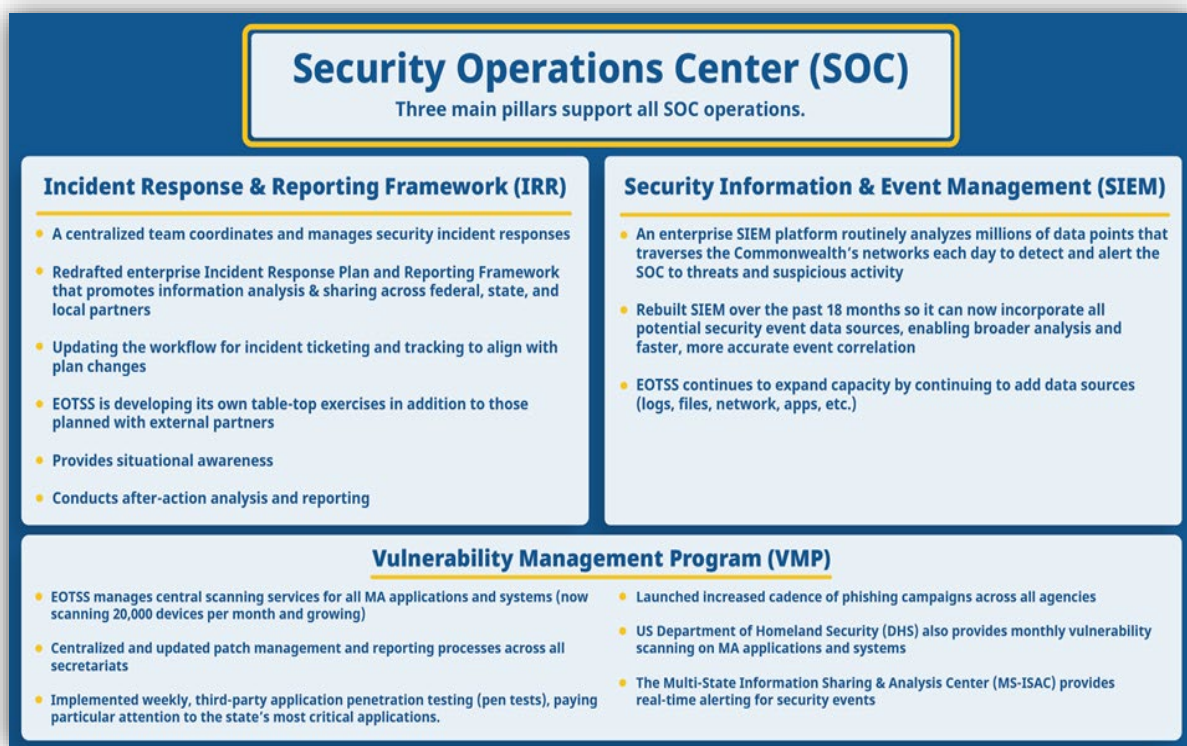
Recent Investments & Accomplishments

In its first years as a secretariat, EOTSS has focused on low-input, high-impact investments 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, and 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.

The Commonwealth Security Operations Center

Most recently, EOTSS has built (and continues to build) out the capacity and services of our enterprise Security Operations Center (SOC) and its Incident Response & Reporting Framework (IRR), Security Incident Event Management (SIEM) system, and Vulnerability Management Program (VMP).

Security Operations Center (SOC)
Three main pillars support all SOC operations.

Incident Response & Reporting Framework (IRR)

- A centralized team coordinates and manages security incident responses
- Redrafted enterprise Incident Response Plan and Reporting Framework that promotes information analysis & sharing across federal, state, and local partners
- Updating the workflow for incident ticketing and tracking to align with plan changes
- EOTSS is developing its own table-top exercises in addition to those planned with external partners
- Provides situational awareness
- Conducts after-action analysis and reporting

Security Information & Event Management (SIEM)

- An enterprise SIEM platform routinely analyzes millions of data points that traverses the Commonwealth's networks each day to detect and alert the SOC to threats and suspicious activity
- Rebuilt SIEM over the past 18 months so it can now incorporate all potential security event data sources, enabling broader analysis and faster, more accurate event correlation
- EOTSS continues to expand capacity by continuing to add data sources (logs, files, network, apps, etc.)

Vulnerability Management Program (VMP)

- EOTSS manages central scanning services for all MA applications and systems (now scanning 20,000 devices per month and growing)
- Centralized and updated patch management and reporting processes across all secretariats
- Implemented weekly, third-party application penetration testing (pen tests), paying particular attention to the state's most critical applications.
- Launched increased cadence of phishing campaigns across all agencies
- US Department of Homeland Security (DHS) also provides monthly vulnerability scanning on MA applications and systems
- The Multi-State Information Sharing & Analysis Center (MS-ISAC) provides real-time alerting for security events

The SOC is a centralized operations center for the Executive Branch that addresses security issues on an organizational and technical level. It is built to identify, protect, detect, respond to, and recover from cyber incidents across the Commonwealth.

Through the IT Capital Investment Plan, EOTSS increased SOC capacity and services to implement 24x7x365 operations to support the enterprise and to continue building out monitoring, alerting and mitigation of threats.

SIEM & Vulnerability Management

At the heart of the SOC is SIEM and the Vulnerability Management Program (VMP). Capital investments provided for an enterprise SIEM platform that routinely analyzes millions of data points and traverses the Commonwealth's networks each day to detect and alert the SOC to threats and suspicious activity. EOTSS rebuilt SIEM over the past 18 months so it can now incorporate all potential security event data sources, enabling broader analysis and faster, more accurate event correlation. EOTSS continues to expand capacity by continuing to add data sources (logs, files, network, apps, etc.).

Similarly, VMP investments now allow EOTSS to centrally manage scanning services for all MA applications and systems. 20,000 devices are scanned per month (and growing). Patch management and reporting processes have also been centralized and updated across all secretariats.

Investments have also enabled weekly, third-party application penetration testing (pen tests) and increased the cadence of phishing campaigns across all agencies. To augment these services, EOTSS contracts with the US Department of Homeland Security (DHS) to provide monthly vulnerability scanning on MA applications and systems and with the Multi-State Information Sharing & Analysis Center (MS-ISAC) provides real-time alerting for security events.

Security Incident Response & Reporting

In 2021, EOTSS led a comprehensive review and update of the Enterprise Security Incident Response & Reporting Framework (IRR) for the Executive Branch. The IRR is the third key component of our unified enterprise security operations.

Changes to the IRR were memorialized in a recent [Administrative Directive](#) from the EOTSS Secretary Under the updated IRR, a centralized team at EOTSS coordinates and manages security incident responses. This team includes (but is not limited to) the EOTSS Secretary; the Assistant Secretary for Technology, Security, and Operations; the Chief Information Security Officer; and the Director of Security Operations.

Last year, this team redrafted the Enterprise Incident Response Plan and Reporting Framework that promotes information analysis & sharing across federal, state, and local partners, and it updated the workflow for incident ticketing and tracking to sync with plan changes.

The new IRR promotes better collaboration and communication among federal, state, and local partners. It enhances situational awareness and improves after-action analysis and reporting for incidents. The updated framework also improved information sharing, planning, and outreach with these partners through regular working group sessions and table-top exercises, as well as provided information on securing critical infrastructure across the Commonwealth.

Cybersecurity Awareness Training & Phishing Campaigns

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.

Additionally, 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 2022, EOTSS facilitated a new round of Municipal Cybersecurity Awareness Grants to provide this critical training to more of the Commonwealth's municipal and state higher education institutions.

Enterprise Risk Management

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.

Cybersecurity & Enterprise Risk Management: FY23-FY25

Preparation for cyber threats is an ongoing and hyper-focused effort. It is critical for the Commonwealth to remain in a state of readiness and preparedness to best position itself to mitigate potential cyber threats and maintain continuity of government services for the customers and constituents we serve.

For FY23-FY25, EOTSS is firmly committed to partnering with the Administration, the Legislature, and its fellow secretariats to make additional investments in the people, processes, and technologies that drive the state's security operations, risk management, and data privacy efforts.

Cybersecurity & Risk Management Priorities:

1. **SOC Investments:** Continue the investment in and build out of the Commonwealth's enterprise Security Operations Center (SOC) services and refine the updated incident reporting and response framework to improve upon cybersecurity situational awareness, readiness, and preparedness across the enterprise.

2. **Cybersecurity Modernization:** Continue the modernization of the Commonwealth's security technology - including advanced monitoring analytics and automation services – to ensure that Massachusetts can protect against today's bad actors and the emerging threats of tomorrow.

3. **Training, Phishing, And Tabletops:** Target new investments to expand end user education, security awareness training, phishing campaigns, and table-top exercises across the enterprise.

4. **Cyber Disruption Team:** Increase the Commonwealth's capacity in the newly formed Cyber Disruption Program and strengthen the skill sets of the Cyber Disruption Team members.

5. **Governance, Risk, and Compliance:** Expand the Commonwealth's governance, risk, and compliance programs by rolling out the EOTSS vendor policy and compliance program, launching the vendor risk portal, and adopting StateRAMP standards and best practices.

6. **Cybersecurity and Resiliency Trust Fund:** Establish and initially fund the Cybersecurity and Resiliency Trust Fund recommended by the Governor in his FY23 budget recommendations to support the procurement of end-user devices and the Modern Workplace Program administered by EOTSS.

7. **Federal Cybersecurity Grants for State and Local Governments:** Complete the state cybersecurity plan and issue grants to state and local governments to modernize legacy IT systems and enhance their cybersecurity posture – via guidance and funding included in the Infrastructure Investment and Jobs Act (IIJA).

Enterprise Network, Core IT Infrastructure, & Hosting

Along with strengthening the Commonwealth's cybersecurity posture, EOTSS' other main objective has been the deployment of a Standard Operating Environment (SOE) with a consistent technology architecture across the Executive Branch.

Historically, IT infrastructure and services were organized at the individual secretariat and agency level in the Commonwealth. Secretariats maintained their own strategic network objectives, deployed a disparate array of technology services and solutions, and hosted most business applications, systems, and infrastructure in aging, on-premises agency data centers or other state-owned facilities.

The Administration established EOTSS to tackle the logistical challenges and security concerns evident in the previous, decentralized model. Since then, the Commonwealth has recognized the importance of supporting investments in modernizing its IT infrastructure and further centralizing enterprise IT management and service delivery under EOTSS.

To achieve its goal of deploying a SOE with a consistent technology architecture, EOTSS made critical investments in the modernization of enterprise network and IT infrastructure and the migration of legacy applications and systems from state-run data centers to contemporary third-party hosting solutions – including cloud services.

These investments set the Commonwealth on the path towards unified networking, infrastructure, and hosting standards that ensure resiliency, redundancy, and business applications availability.

One Network

To address the concerns and challenges of having different secretariat and agency networks scattered across the enterprise, EOTSS launched the One Network initiative in 2019.

One Network is a cross-secretariat program involving all Executive Branch state agencies aimed at folding all secretariats and agencies into a single core network operated by EOTSS. The core network serves as the foundation for all Commonwealth information services including e-mail, data center operations, network communications, business applications, and internet service.

One Network Phase I Objectives

1 Resolve security concerns by migrating all internet ingress and egress at the secretariat level to the center, so that EOTSS could control and monitor network traffic leveraging enterprise infrastructure and security tools.

2 Inventory the private IP addresses in use, create an enterprise private IP address management strategy, and eliminate any overlap that existed within the Executive Branch amongst the nine secretariats.

Phase I was completed in 2020. As part of phase I, EOTSS migrated all internet ingress and egress at the secretariat level to the center, so that EOTSS could control and monitor network traffic leveraging enterprise infrastructure and security tools. EOTSS then inventoried private IP addresses in use, created an enterprise private IP address management strategy, and eliminated unnecessary redundancies.

These two objectives set the foundation for the recent redesign and build out of the Commonwealth's core network into contemporary, privately-managed data centers over the past 18 months – as well as for wide area network (WAN) optimization efforts and the long-term IP address strategy.
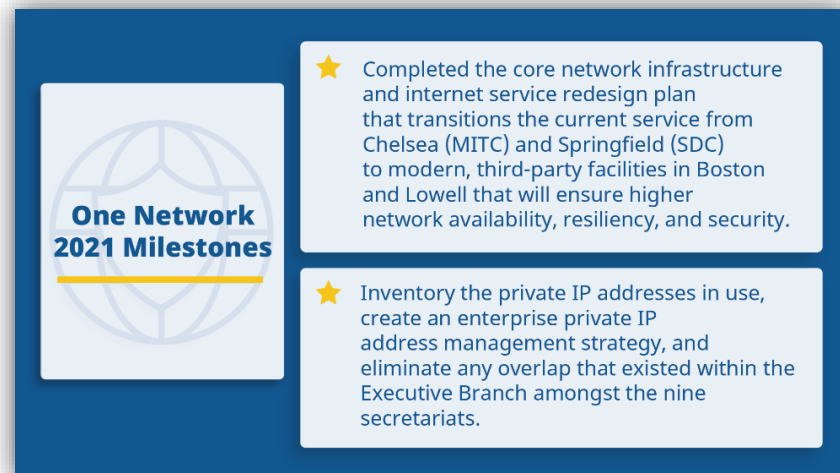
Phase II was completed in 2021. As part of phase II, EOTSS finished the core network infrastructure and internet service redesign plan that transitions the current service from Chelsea (MITC) and Springfield (SDC) to third-party co-located facilities in Boston and Lowell that will ensure higher network availability, resiliency, and security. EOTSS also procured the new primary and secondary network infrastructure locations to support the upcoming transition to new facilities.

Infrastructure & Hosting

In October of 2019, the EOTSS Secretary implemented a significant policy change for infrastructure hosting (Cloud, Services, Migration) and transitioned from a "cloud first" approach with a single provider to a "cloud smart" model utilizing hybrid/multi-cloud hosting solutions.

In 2020 and 2021, EOTSS also accelerated the closure of state-owned data centers and moved towards a private-public cloud environment offering a more resilient and reliable infrastructure for agency business applications and services. Software as a Service (SaaS) platforms, Infrastructure as a Service (IaaS), and managed services were also encouraged by EOTSS for many critical needs as part of this transformation.

Today, EOTSS offers multiple cloud offerings and hosting solutions – Hybrid Cloud, On-premises, 3rd-Party Hosting, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-service (SaaS). Agencies are now relying less on state-owned data centers and moving infrastructure to modern hosting environments and state-of-the-art facilities.

Since 2017, EOTSS has coordinated the migration of almost 400 Commonwealth applications and platforms to the new model – including 99 applications this past year alone. Recent examples include, but are not limited to:

- HR/CMS

- Commonwealth Information Warehouse (CIW)

- DPH Mass Immunization Information System

- DPH Electronic Disease Surveillance System

- EOHHS Health Information Exchange

- DDS Home and Community Services Information System

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, more 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.

Application Rationalization

While EOTSS assumed oversight of core IT and cybersecurity infrastructure and services, the management of the business application layer was preserved at the agency and secretariat level where there resides deep subject matter expertise and knowledge of an application's role and impact with respect to daily operations.

However, agencies are actively working with EOTSS on the enterprise Application Rationalization program – where SCIOs strategically identify their critical legacy application footprint and decide which should be kept, replaced, retired, or consolidated. Action items are prioritized over a three to five-year time horizon as part of the SCIO IT strategic planning process.

Once prioritized, applications remaining in service are migrated to approved hosting options referenced above.

Consolidated Active Directory

EOTSS is implementing an enterprise-wide Azure Active Directory to consolidate numerous on-premises forests/domains into an enterprise forest within Azure – with Multi-Factor Authentication (MFA) enabled.

The Azure Active Directory (AD) Identity Access Management (IAM) framework supports strategic and tactical goals of promoting government business and technical resiliency, offering enhanced citizen experiences, and enabling the state workforce with a modern and mobile technology platform in support of good government.

To date, the efforts have focused on eliminating redundant and often competing technologies, and with the adoption of the Azure AD framework as the enterprise standard, the move to retire previous IAM platforms was prioritized. This program began in 2019 and will be completed with the full migration off the legacy system in FY23.

Legacy Mainframe Reduction

EOTSS is in the process of retiring the on-premise mainframe environment. One of the largest mainframe customer agencies was able to completely move off the legacy mainframe in 2020-2021, and EOTSS is working on a plan to retire the few remaining applications in FY23-24.

Network, Core Infrastructure & Hosting: FY23-25

EOTSS remains committed to its enterprise goals of retiring old infrastructure and mainframes, moving out of state-owned data centers, and migrating applications and systems to approved hosting solutions as part of the SOE framework.

We have adapted our infrastructure hosting approach to include public-private cloud environments that meet todays and tomorrow's environmental standards and practices, while also providing the Commonwealth with better resiliency, immediate scalability, and higher availability.

Maintaining a SOE with a consistent, well-defined approach to budgeting, spending, technology architecture, service delivery and technical support provides for the greatest opportunity to ensure that Commonwealth systems remain available and secure for our agencies and constituents.

<u>**One Network, Core Infrastructure & Hosting Priorities:**</u>

1. **One Network Infrastructure:** Complete Commonwealth One Network infrastructure move to secure, 3rd party co-located facility with modern and highly redundant power and cooling measures, as well as built-in disaster recovery features with geographic diversity.

2. **WAN Buildout and Optimization:** Build out the wide area network (WAN) and security services to account for and support increased resiliency, mobility, and remote management within the Commonwealth Core Network (One Network).

3. **Active Directory (AD) Consolidation:** Complete consolidation of Active Directory (AD) domains across 3 remaining secretariats and mitigate IP addressing conflicts.

4. **One Network Consolidation:** Collapse 3 remaining agency networks into the Commonwealth One Network operation.

5. **Closing State-run Data Centers:** Finalize plan to migrate remaining agency business applications, mainframes, and systems out of the Chelsea and Springfield state-run data centers to approved public-private cloud hosting environments.

6. **Platform and Architecture Models:** Finalize Cloud Hosting Platform and Infrastructure Architecture Models for publication as part of the EOTSS Standard Operating Environment.

7. **Application Rationalization:** Continue to work with agency partners to identify and prioritize opportunities for further application migrations to the cloud, 3rd party co-located facilities, or other EOTSS-approved hosting solutions (PaaS, SaaS, and IaaS).

Digital & Data Services

The EOTSS Digital and Data Offices set the enterprise policies, standards, and guidelines for their respective subject matter areas in coordination with the EOTSS Secretary and Commonwealth CIO.

More importantly, they seek to help their partners use the best technology, design, and data to make every interaction with Massachusetts government simpler, faster, and more meaningful. They achieve their missions by collaborating with organizations across state government to improve the constituent digital experience and transform how residents, visitors, businesses, and government agencies interact with the Commonwealth.

MA Digital and Data Services

With the establishment of EOTSS in 2017, the EOTSS Secretary named the Commonwealth's first Chief Digital & Data Officer (CDO), and MA Digital & Data Services was born.

The team then embarked on an enterprise-wide digital transformation aimed at overhauling the legacy Commonwealth internet presence and replacing it with a new Mass.gov web platform. They also built out an organization to develop processes, standards, and solutions that make it easier for agencies to digitally deliver critical government services and information to their constituents.

Mass Digital assists agencies throughout the entire digital project life cycle – from initial whiteboard sessions through to go-live. The team offers (among other services):

- Content Design & Writing to help create, edit, and optimize content – as well as to assist with digital marketing campaigns, search engine optimization, information architecture and social media.

- Video & Multimedia services such as live action videos, interviews, and motion graphic explainer videos. They also offer traditional photography and some audio recording services.

- Web Analytics services to help agencies gain more insight into how people engage with their content.

- Web Design services that help agencies build an easy-to-use, modern, accessible website to deliver their services.

To further assist agencies and content editors across the enterprise with their digital projects, the Digital Team created the Mayflower open source design system and the Mass.gov Knowledge Base. Together, these tools provide self-service guides, tips, and best practices for authoring and updating content for Mass.gov and state web applications.

Since 2019, they have overseen the creation of nearly 70,000 Mass.gov webpages generating more than 960 million pageviews across the platform.

Digital Engagements & COVID-19

2019 saw an increased demand for core digital and data service offerings, as well as in cross-secretariat and cross-agency engagements. Over the past 2+ years, they have participated in 28 separate engagements with agency partners across the enterprise.

Examples include collaboration with the Executive Office of Labor and Workforce Development (EOLWD) on the creation of digital content and strategies for the Department of Family and Medical Leave (DFML) and the rollout for the [Commonwealth's Paid Family and Medical Leave system](#) and significant efforts to assist in the Commonwealth's COVID-19 response.

Among the team's COVID-19 efforts were the development and rollout of critical COVID testing and vaccine websites and supporting systems (such as chatbots). Examples of these websites and systems include:

- [COVID-19 Testing Sites](#)

- [COVID-19 Vaccine Finder](#)

- [Vaccine Pre-Registration & Notification System](#)

- [Massachusetts Digital Vaccine Card](#) and [My Vax Records](#)

Data Office & Data Privacy

Since 2018, the Commonwealth has made great strides in building and improving on the legal and technical infrastructure necessary to facilitate data-driven government.

The Chief Data Officer (CDO) for the Commonwealth oversees the EOTSS Data Office and is responsible for developing and governing the enterprise data and information strategy and facilitating data sharing amongst state agencies and the public. The CDO develops and maintains data procedures and policies, seeks to improve and streamline data systems within the organization, and drives innovation in the area of enterprise-wide data and analytics.

In 2019, the EOTSS Secretary appointed the Commonwealth's first Chief Privacy Officer (CPO) to strengthen enterprise leadership around data privacy and [information governance](#). The CPO works specifically to establish privacy and security frameworks to protect the dissemination of sensitive data and to resolve data privacy and security concerns.

The position works closely with the CDO and Data Office to review and offer feedback on data sharing agreements between state agencies. The CDO and CPO also support engagement with the Data Steward Council that was formed in 2018 in discussions of data sharing policies and data goals among executive branch agencies. Their combined efforts facilitate the deliberate and thoughtful use of data across agencies to inform policy choices and agency strategy.

Enterprise Data Projects

Since October 2018, the Data Office has commenced and completed several multi-agency data-sharing projects. Early projects included the creation of [public-facing data sites](#) to meet the Department of Public Utilities' (DPU) statutory reporting requirements for transportation network companies (TNCs) and the 2019 effort with the Department of Transitional Assistance (DTA) to help address ["churn" among SNAP recipients](#).

In addition to playing a critical role in supporting the state's COVID-19 response and cross-secretariat engagements (as outlined in other sections of this report), more recent Data Office accomplishments include:

- [Learn to Earn](): This ten-agency initiative was launched by the Governor's Office to make available de-identified, aggregated data about common clients of transitional assistance programs and how they progress towards economic stability.

- [Early Childhood Integrated Data System (ECIDS)](): In 2020-2021, the Data Office stood up an architecture that intakes data from seven Education and Health and Human Services agencies providing early childhood development programs and (for the first time) matches individual participants across programs to analyze patterns in how families utilize birth-5 programming by demographics, areas where families may be underserved, and how program participants perform on grades K-3 success metrics.

- [HRD Diversity Dashboard](): Built and launched a public-facing dashboard of the Commonwealth's workforce focused on time trends and demographics. The product improved data transparency and allowed state agencies and the public to self-serve the data, cutting down the time HRD spends servicing internal and external reporting and information requests. Phase II, slated for completion in late 2022, will extend the product to employment flows – including hires, promotions, transfers, and terminations.

- [Differential Privacy:]() From Oct 2021-Feb 2022, the Data Office worked in conjunction with MIT Lincoln Labs to adapt and implement a set of innovative statistical privacy tools developed at Harvard and explore their applications within administrative datasets to reduce barrier to data sharing and allow for more detailed and robust internal and public data reporting, while reducing risks to individual privacy. A pilot implementation focused on early childhood development programs is underway to evaluate applicability.

Lastly, the Data Office just launched the first phase of the Commonwealth's new [Data Hub](). This mass.gov portal offers new categorization and improved search functionality to help users more quickly and easily locate data published by state agencies on and off mass.gov. The Team has worked with 60+ agencies (and counting) to improve the content on their data pages, and to cross link data sets by topic to allow for broader search capabilities, eliminating the need for a constituent to be an expert on where certain data sets are kept, and by which agency.

Digital & Data Services: FY23-25

Since 2017, the Commonwealth has made great strides in improving the constituent digital experience and transforming how residents, visitors, businesses, and government agencies interact with government.

Moreover, the Executive Branch has developed and maintained a robust data and information strategy to facilitate data sharing amongst state agencies and the public. Agencies are using data and data analytics to make more informed decisions with respect to policy choices, programs, and constituent services.

The pandemic has reinforced the importance of citizen-centric digital services to increase access to essential services and ensure the continuity of government operations. COVID-19 also heightened interest in and the use of data analytics in agency decision making, communications, and policy choices.

Digital & Data Services Priorities:

1. **Digital & Data Roadmap:** Develop and publish an updated roadmap for the Commonwealth's Digital and Data strategies over the next three years.

2. **Enhance Digital Service Standards:** Raise Digital Service standards as technologies get upgraded and transform the user experience for constituents through cross-agency engagements. Current engagements include:
   a. Unemployment modernization (2022-2024).
   b. Integrated Eligibility and Enrollment for food assistance and Medicaid (2022-2024).

3. **Multilingual Interactions:** Improve multilingual interactions across state web properties leveraging correctable machine translation.

4. **Enterprise Chatbot:** Develop and deploy enterprise chatbot for all of Mass.gov and expand the use of Artificial Intelligence (AI) – to include virtual assistants, voice recognition and commands.

5. **Open Data:** Continue to build out the Commonwealth's open data program, including enterprise-wide standards for publishing data, and the availability of high-quality, machine-readable datasets.

6. **Criminal Justice Data:** Develop a data system that tracks individuals across their touchpoints with the state's criminal justice agencies and the Trial Court and captures key patterns and outcomes.

7. **Data Governance:** Further build and expand enterprise data governance efforts at the secretariat level, including the development of cross-agency data lakes, and ensure efforts are coordinated to allow for frictionless data sharing across secretariats.

8. **Data Steward Council:** Continue efforts of Data Steward Council and program priorities and expand the development of data privacy standards and tools at the enterprise level.

9. **Data Analytics:** Expand the Data Analytics program into a more formal application-based process whereby agencies can apply to EOTSS for business intelligence funding as well as services.

10. **Business Intelligence:** Implement a business intelligence training program and workshop series for agency personnel to expand their ability to report and use data effectively.

Enterprise Programs & Strategic Engagements

As the lead enterprise IT organization for the Executive Branch, EOTSS seeks to improve and promote better service delivery to its constituent agencies.

EOTSS works toward this goal by making investments in the development and deployment of centrally managed programs that more efficiently deliver solutions through modern technologies, enterprise leadership and expertise, and economies of scale.

Examples include e-Discovery, Enterprise Print Services, Contract Management Office & Enterprise Software Licensing, IT Accessibility, and Customer Engagement (among others highlighted in the EOTSS 2022 Annual Report).

EOTSS also offers guidance, project management, and support to other agencies through strategic engagements that seek to increase the efficiency and responsiveness of state agencies by improving service delivery and adopting new technology-enabled business solutions.

A consulting team from the EOTSS Office of Strategy Management (OSM) often takes the lead and pulls in other divisions and subject matter experts as needed depending on the scope of the engagement.

These efforts are true partnerships between the agency business and IT organizations as they work with the Strategy Team to define the problem, redesign business processes, oversee procurements, and manage the technology implementations. Recent examples include engagements on Paid Family and Medical Leave (PFML) and the Department of Family and Medical Leave (DFML).

Demand for Strategy Services has increased steadily over the last several years. Through the team's collaboration with partner agencies, EOTSS has gained success in influencing and directing agencies to make smarter choices and better decisions in technology procurements.

Enterprise Programs & Strategic Engagements: FY23-FY25

1. **Enterprise Voice Platform:** Rollout the next generation of the Enterprise Voice Platform (MassVoice) – a cloud-based enterprise managed voice solution – to all executive branch agencies, establishing one unified communications solution for the enterprise.

2. **Enterprise Print Rollout:** Complete the rollout of the Enterprise Print Services Platform to all Executive Branch agencies – a vendor-agnostic, software-driven solution that provides for a centrally-managed, secure service for on premise and remote printing.

3. **e-Discovery Expansion:** Expand the capacity and capabilities of the e-Discovery Team to meet increasing demand for enterprise software capable of ingesting large volumes of electronic data from multiple sources beyond email data, such as desktop applications and network share drives.

4. **Contract Management Office & Enterprise Software Licensing Expansion:** Expand the capacity and engagement of the Contract Management Office to enhance consulting on enterprise-wide IT contracts, software licensing, contract/licensing compliance, Cloud Services, Software as a Service (SaaS), and overall IT procurement support/guidance to other state agencies.

5. **Customer and Service Engagement Enhancement:** Complete the Customer and Service Engagement Enhancement Program to increase transparency around EOTSS service offerings and costs, ensure service offerings match customer needs, and promote greater trust and satisfaction through an improved customer experience and fulfillment.

6. **IT Accessibility Roadmap:** Complete a 3-year IT Accessibility Roadmap to establish program priorities and to chart out the next phase of the EOTSS IT Accessibility Enterprise strategy and service offerings.

IT Capital Investment Plan

EOTSS oversees the IT capital investment portfolio and related program management through its Office of Capital Planning. The EOTSS Secretary in collaboration with the IT Investment Advisory Board (IIAB), reviews and recommends projects to the Governor and the Secretary for Administration & Finance (A&F) for inclusion in the annual Capital Investment Plan (CIP).

As the stewards of IT capital investments, EOTSS and the IIAB have implemented an enterprise framework that promotes standardization and consistency across the Executive Branch. The framework drives overall IT investment strategy and works towards the long-term goals of modernizing legacy IT infrastructure, ensuring the continuity of government services, improving constituent-centric digital services, and enhancing the state's cybersecurity posture.

The individual programs and projects that emerge from the high-level priorities and objectives outlined in this IT Strategic Plan for the Commonwealth and secretariat IT Strategic Plans are submitted for capital funding consideration each year as part of the IT capital Planning Process.

Through this framework, EOTSS brings together leadership from both an agency's business and IT organization to develop a mutual understanding of the business case for a project and to set expectations for the planning process and desired outcomes. These efforts promote communication and collaboration, help establish and manage priorities for the agencies and specific projects and reinforce the enterprise standard operating environment.

The Commonwealth's robust IT capital planning history and established capital funding framework helped establish the foundation for the transformation of IT infrastructure and service delivery for 25+ years. The FY23-27 IT Capital Investment Plan continues this tradition.

Highlights from the FY23-27 IT plan include:

1. **Improving government performance ($78.6 million):** The capital plan provides funding to maintain support for innovative technology solutions that improve operational efficiency in state government.

   The FY23 plan continues to invest in key initiatives such as: the digitization of patient health records at the Holyoke and Chelsea Soldiers' Homes and Departments of Public and Mental Health; the modernization of Trial Courts technical infrastructure to improve litigation processing and enhance the security; the standardization of data collected by the Executive Office of Education and its agencies to connect business applications, streamline user access, and make the data and analytics secure, cloud-based and user-friendly for parents, educators, schools and community education providers; and establishment of a cross-tracking system to consolidate data from criminal justice agencies, trial court, parole, houses of correction and county jails per the recent Criminal Justice Reform Law.

2. **Improving government service delivery ($48.1 million):** EOTSS leads and oversees ongoing IT transformation initiatives across the Commonwealth, with a focus on supporting each agency's efforts to improve the experience of constituents accessing government services.

In FY23, priorities include: modernizing the Commonwealth's Unemployment Insurance online claims system; creating an integrated benefits portal that allows citizens to access multiple health care benefits; expanding electronic access to occupational licenses and permits at EOEEA and EOHED; and the continuing improvements to the Mass.gov data taxonomy that allows citizens to access data and research across all government agencies with one query.

3. **Modernizing technical infrastructures ($27.5 million):** EOTSS will continue to make investments in digital infrastructure, networks, and hosting services to enhance the resiliency of the Commonwealth's information systems and business applications, ensuring the uninterrupted delivery of government services to constituents and stakeholders, and expanding the capabilities of an increasingly mobile workforce.

4. **Securing the integrity of citizen data and state assets ($11.3 million):** The capital plan maintains funding for the Commonwealth's Security Incident and Event Management system, which enhances the security of the Commonwealth's networks and information systems by enabling EOTSS to detect, investigate, communicate, and mitigate cyber threats to systems and data. Another critical component of the Commonwealth's cyber security framework is EOTSS' vulnerability management and mitigation program. This program helps ensure that EOTSS and state agencies remain vigilant and aware of persistent cyber threats and committed to a continuous and adaptive vulnerability management program to mitigate ever-present threats.

5. **Municipal Cybersecurity Awareness Grants**: In addition to the Commonwealth's workforce, EOTSS supports municipal government partners. 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. The FY23 capital plan supports a new round of Municipal Cybersecurity Awareness Grants to continue this critical training for more of the Commonwealth's municipal and state higher education institutions.

Summary of Strategic Plan Priorities

Please find a summary below of the Commonwealth's FY23-25 Priorities as outlined in this Strategic IT Plan for all Executive Branch agencies.

Modern Workplace Program Priorities:

1. **Complete Remaining Workstreams:** Complete the small number of remaining device deployments and file migrations.

2. **Optimize O365 and Azure:** Ensure the Commonwealth is fully leveraging the capabilities of the cloud-based Microsoft Office 365 suite and the Azure Active Directory (AD) framework to support the strategic and tactical goals of promoting government business continuity and technical resiliency.

Cybersecurity & Enterprise Risk Management Priorities:

1. **SOC Investments:** Continue the investment in and build out of the Commonwealth's enterprise Security Operations Center (SOC) services and refine the updated incident reporting and response framework to improve upon cybersecurity situational awareness, readiness, and preparedness across the enterprise.

2. **Cybersecurity Modernization:** Continue the modernization of the Commonwealth's security technology - including advanced monitoring analytics and automation services – to ensure that Massachusetts can protect against today's bad actors and the emerging threats of tomorrow.

3. **Training, Phishing, And Tabletops:** Target new investments to expand end user education, security awareness training, phishing campaigns, and table-top exercises across the enterprise.

4. **Cyber Disruption Team:** Increase the Commonwealth's capacity in the newly formed Cyber Disruption Program and strengthen the skill sets of the Cyber Disruption Team members.

5. **Governance, Risk, and Compliance:** Expand the Commonwealth's governance, risk, and compliance programs by rolling out the EOTSS vendor policy and compliance program, launching the vendor risk portal, and adopting StateRAMP standards and best practices.

6. **Cybersecurity and Resiliency Trust Fund:** Establish and initially fund the Cybersecurity and Resiliency Trust Fund recommended by the Governor in his FY23 budget recommendations to support the procurement of end-user devices and the Modern Workplace Program administered by EOTSS.

7. **Federal Cybersecurity Grants for State and Local Governments:** Complete the state cybersecurity plan and issue grants to state and local governments to modernize legacy IT

systems and enhance their cybersecurity posture – via guidance and funding included in the Infrastructure Investment and Jobs Act (IIJA).

One Network, Core Infrastructure & Hosting Priorities

1. **One Network Infrastructure:** Complete Commonwealth One Network infrastructure move to secure, 3rd party co-located facility with modern and highly redundant power and cooling measures, as well as built-in disaster recovery features with geographic diversity.

2. **WAN Buildout and Optimization:** Build out the wide area network (WAN) and security services to account for and support increased resiliency, mobility, and remote management within the Commonwealth Core Network (One Network).

3. **Active Directory (AD) Consolidation:** Complete consolidation of Active Directory (AD) domains across 3 remaining secretariats and mitigate IP addressing conflicts.

4. **One Network Consolidation:** Collapse 3 remaining agency networks into the Commonwealth One Network operation.

5. **Closing State-run Data Centers:** Finalize plan to migrate remaining agency business applications, mainframes, and systems out of the Chelsea and Springfield state-run data centers to approved public-private cloud hosting environments.

6. **Platform and Architecture Models:** Finalize Cloud Hosting Platform and Infrastructure Architecture Models for publication as part of the EOTSS Standard Operating Environment.

7. **Application Rationalization:** Continue to work with agency partners to identify and prioritize opportunities for further application migrations to the cloud, 3rd party co-located facilities, or other EOTSS-approved hosting solutions (PaaS, SaaS, and IaaS).

Digital & Data Priorities

1. **Digital & Data Roadmap:** Develop and publish an updated roadmap for the Commonwealth's Digital and Data strategies over the next three years.

2. **Enhance Digital Service Standards:** Raise Digital Service standards as technologies get upgraded and transform the user experience for constituents through cross-agency engagements. Current engagements include:
   a. Unemployment modernization 2022-2024.
   b. Integrated Eligibility and Enrollment for food assistance and Medicaid 2022-2024.

3. **Multilingual Interactions:** Improve multilingual interactions across state web properties leveraging correctable machine translation.

4. **Enterprise Chatbot:** Develop and deploy enterprise chatbot for all of Mass.gov and expand the use of Artificial Intelligence (AI) – to include virtual assistants, voice recognition and commands.

5. **Open Data:** Continue to build out the Commonwealth's open data program, including enterprise-wide standards for publishing data, and the availability of high-quality, machine-readable datasets.

6. **Criminal Justice Data:** Develop a data system that tracks individuals across their touchpoints with the state's criminal justice agencies and the Trial Court and captures key patterns and outcomes.

7. **Data Governance:** Further build and expand enterprise data governance efforts at the secretariat level, including the development of cross-agency data lakes, and ensure efforts are coordinated to allow for frictionless data sharing across secretariats.

8. **Data Steward Council:** Continue efforts of Data Steward Council and program priorities and expand the development of data privacy standards and tools at the enterprise level.

9. **Data Analytics:** Expand the Data Analytics program into a more formal application-based process whereby agencies can apply to EOTSS for business intelligence funding as well as services.

10. **Business Intelligence:** Implement a business intelligence training program and workshop series for agency personnel to expand their ability to report and use data effectively.

Enterprise Programs & Strategic Engagement Priorities

1. **Enterprise Voice Platform:** Rollout the next generation of the Enterprise Voice Platform (MassVoice) – a cloud-based enterprise managed voice solution – to all executive branch agencies, establishing one unified communications solution for the enterprise.

2. **Enterprise Print Rollout:** Complete the rollout of the Enterprise Print Services Platform to all Executive Branch agencies – a vendor-agnostic, software-driven solution that provides for a centrally-managed, secure service for on premise and remote printing.

3. **e-Discovery Expansion:** Expand the capacity and capabilities of the e-Discovery Team to meet increasing demand for enterprise software capable of ingesting large volumes of electronic data from multiple sources beyond email data, such as desktop applications and network share drives.

4. **Contract Management Office & Enterprise Software Licensing Expansion:** Expand the capacity and engagement of the Contract Management Office to enhance consulting on enterprise-wide IT contracts, software licensing, contract/licensing compliance, Cloud Services, Software as a Service (SaaS), and overall IT procurement support/guidance to other state agencies.

5. **Customer and Service Engagement Enhancement:** Complete the Customer and Service Engagement Enhancement Program to increase transparency around EOTSS service offerings and costs, ensure service offerings match customer needs, and promote greater trust and satisfaction through an improved customer experience and fulfillment.

6. **IT Accessibility Roadmap:** Complete a 3-year IT Accessibility Roadmap to establish program priorities and to chart out the next phase of the EOTSS IT Accessibility Enterprise strategy and service offerings.

IT Capital Investment Plan Priorities

1. **Improving government performance ($78.6 million):** The capital plan provides funding to maintain support for innovative technology solutions that improve operational efficiency in state government.

   The FY23 plan continues to invest in key initiatives such as: the digitization of patient health records at the Holyoke and Chelsea Soldiers' Homes and Departments of Public and Mental Health; the modernization of Trial Courts technical infrastructure to improve litigation processing and enhance the security; the standardization of data collected by the Executive Office of Education and its agencies to connect business applications, streamline user access, and make the data and analytics secure, cloud-based and user-friendly for parents, educators, schools and community education providers; and establishment of a cross-tracking system to consolidate data from criminal justice agencies, trial court, parole, houses of correction and county jails per the recent Criminal Justice Reform Law.

2. **Improving government service delivery ($48.1 million):** EOTSS leads and oversees ongoing IT transformation initiatives across the Commonwealth, with a focus on supporting each agency's efforts to improve the experience of constituents accessing government services.

   In FY23, priorities include: modernizing the Commonwealth's Unemployment Insurance online claims system; creating an integrated benefits portal that allows citizens to access multiple health care benefits; expanding electronic access to occupational licenses and permits at EOEEA and EOHED; and the continuing improvements to the Mass.gov data taxonomy that allows citizens to access data and research across all government agencies with one query.

3. **Modernizing technical infrastructures ($27.5 million):** EOTSS will continue to make investments in digital infrastructure, networks, and hosting services to enhance the resiliency of the Commonwealth's information systems and business applications, ensuring the uninterrupted delivery of government services to constituents and stakeholders, and expanding the capabilities of an increasingly mobile workforce.

4. **Securing the integrity of citizen data and state assets ($11.3 million):** The capital plan maintains funding for the Commonwealth's Security Incident and Event Management system, which enhances the security of the Commonwealth's networks and information systems by enabling EOTSS to detect, investigate, communicate, and mitigate cyber threats to systems and data. Another critical component of the Commonwealth's cyber security framework is EOTSS' vulnerability management and mitigation program. This program helps ensure that EOTSS and state agencies remain vigilant and aware of persistent cyber threats and committed to a continuous and adaptive vulnerability management program to mitigate ever-present threats.

5. **Municipal Cybersecurity Awareness Grants**: In addition to the Commonwealth's workforce, EOTSS supports municipal government partners. 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. The FY23 capital plan supports a new round of Municipal Cybersecurity Awareness Grants to continue this critical training for more of the Commonwealth's municipal and state higher education institutions.

Appendix

EOTSS Statutory Authority

- [Chapter 64 of the Acts of 2017](#)

- [M.G.L. c. 6A, s. 7A](#)

- [M.G.L. c. 7D](#)

EOTSS Policies, Standards, and Guidelines
https://www.mass.gov/info-details/enterprise-policies-standards-guidelines#mass-digital-services-

Pursuant to M.G.L. c. 6A, § 7A, and M.G.L. c. 7D, EOTSS has established policies, standards, and guidelines as part of its Standard Operating Environment (SOE) for the procurement, delivery, and support of information technology systems and services across the Commonwealth's Executive Branch agencies.

Collectively, the policies, standards, and guidelines that make up the SOE help protect the confidentiality, integrity, and availability of the Commonwealth's data and information systems. Agency business and IT leadership are expected to be knowledgeable and compliant with all policies, standards, and guidelines.

Please note: While non-Executive branch agencies are not required to follow defined EOTSS policies, standards, and guidelines, compliance is recommended.

EOTSS 2022 Annual Report
https://www.mass.gov/report/2022-eotss-annual-report

The Commonwealth finds itself at a transformational moment as technology becomes ever-more integrated into the way government conducts business. This annual report serves as an informative resource for our state leaders, public agency partners, and constituents to learn more about EOTSS' role as the lead enterprise information technology (IT) and cybersecurity organization for the Executive Branch.

IT spending reports
EOTSS FY21 $250K+ IT Projects Report
EOTSS FY20 report to the Legislature on Commonwealth IT procurements

All IT-related project expenditures over the previous 12-month period.

Information Governance Framework
https://www.mass.gov/doc/2020-eotss-information-governance-framework/download

This framework provides independent planning, execution, and management of the necessary policies, standards, practices, technologies, and tools to support our information lifecycle, risk, and compliance needs at an enterprise level.

EOTSS News and Announcements

https://www.mass.gov/orgs/executive-office-of-technology-services-and-security/news

- Municipal Fiber Grant program

- Baker-Polito Administration Awards $3.5 Million for Local Technology Infrastructure

- Baker-Polito Administration Hosts 2021 Massachusetts Virtual Digital Government Summit

- Baker-Polito Administration Announces Preregistration System for Mass Vaccination Locations to Launch Friday, Updates on Dose Distribution in the Commonwealth & Designated Vaccine Clinic Days for K-12 Educators, Staff & Child Care Workers

IT Capital Plan and Program Management

- Office of Capital Planning

- FY2022 Capital Investment Plan (CIP)

- FY2023 Capital Investment Plan (CIP)

- 2020 General Government Bond Bill

- IT Investment Advisory Board (IIAB)

- IT Capital Planning Process

EOTSS Fiscal Year 2023 Financials

- FY2022 General Appropriations Act

- FY2022 Appropriations

- FY22 Chargeback Rate Schedule

- EOTSS Chargeback Model

- Governor's FY2023 Budget Recommendations

The Executive Office of Technology Services and Security
McCormack Building - Main Office
1 Ashburton Place, 8th Floor
Boston, MA 02108

Main Office (617) 626-4400
Open Monday through Friday:
8:30 a.m. - 4:30 p.m.