****

**OA-OIT Service Catalog**

**Office of Administration – Office for Information Technology**

**Version 1.7 – September, 2017**

**Table of Contents**

Summary Table 5

Infrastructure as a Service 9

EDC Services 9

EDC Services: Service Request Status 10

Platform as a Service 11

Campus Wireless 11

Enterprise Business Intelligence Suite (Business Objects) 12

Enterprise Messaging 13

Global Managed File Transfer (MFT) 14

Kofax Enterprise E-Fax 15

ListServ 16

SAP Learning Solution – LSO 17

SharePoint Online 18

SharePoint 2013 On-Premises Shared Service 20

Virtual Desktop Services 21

VMware Licensing – Resident Consultant Service 22

Voice & Unified Communications Division (V/UCD) for Enterprise Call Center Services (ECCS) - Genesys 23

Voice & Unified Communications Division (V/UCD) for Enterprise Cisco WebEx Platforms 24

Voice & Unified Communications Division (V/UCD) for Enterprise Mobile Management Services (EMMS) - AirWatch 25

Voice & Unified Communications Division (V/UCD) for Enterprise Verizon/Unify Platforms 26

Web Map Hosting 28

Professional Services 29

Cloud Use Case Review 29

Desktop Support 30

EARC Intake Form 31

Enterprise IT Policy Management 32

LAN Support 33

Voice & Unified Communications for Consolidated Agencies 34

Web Site or Content Development and Support 35

Security Services 36

Advanced Persistent Threat (APT) Protection 36

Application Source Code Scanning Utilizing IBM Rational Appscan 37

Cloud Access Portal (ITP-SEC003 Waiver) 38

Commonwealth User Provisioning and Self-Service (CUPSS) 39

Computer Forensics Investigations 40

COPA Identity Exchange 41

Cyber Security Training & Awareness 42

eDiscovery and Forensics 43

Endpoint Protection 44

Enterprise Directory Services 46

Incident Response and Investigations 47

Information Security Officer - ISO 48

Information Technology Governance, Risk, and Compliance (IT-GRC) Solution 49

Internet Access Compliance and Control Management 51

Perimeter Threat Protection 52

Risk-Based Multi-Factor Authentication (RBMFA) 53

Security Assessment 54

Single Signon 55

Social Engineering Security Awareness Training 56

Vulnerability Management 57

Vulnerability Scanning 58

Web Application Firewall 59

Web Application Vulnerability Scanning 60

Web Content Reporting 61

Software as a Service 62

Address Verification 62

Alerting and Notifications 63

Application Development& Support 64

ArcGIS Desktop Tools 65

Daptiv Project Portfolio Management 66

Geocoding 67

GIS Data Hosting and Metadata 68

IES ERP Business Application Services 69

Information Technology Service Management (ITSM) System 71

OneDrive for Business (OD4B) 73

PA Map Gallery 74

TomTom Tools 75

Web Map Creation 76

|  |
| --- |
| This document describes the services offered by the Office of Administration – Office for Information Technology to commonwealth departments, boards, commissions and councils under the Governor’s jurisdiction.This service catalog is for informational purposes and does not constitute a contract.Planned outages are scheduled in compliance with IT Policy SYM010 – Enterprise Services Maintenance Scheduling. |

# Summary Table

The below table illustrates which services are available to each agency and how agencies initiate the service.

| **Service** | **Provided to All Agencies?** | **Do Agencies Receive Service Automatically or Via Service Request?** |
| --- | --- | --- |
| **Infrastructure as a Service (IaaS)** |
| EDC Services | All Agencies | Service Request |
| EDC Services: Service Request Status | All Agencies | Service Request |
| **Platform as a Service (PaaS)** |
| Campus Wireless | All Agencies | Service Request |
| Enterprise Business Intelligence Suite (Business Objects) | All Agencies | Service Request |
| Enterprise Messaging | All Agencies | Based on CUPPS Provisioning Policies |
| Global Managed File Transfer (MFT) | All Agencies | Service Request |
| Kofax Enterprise E-Fax | All Agencies | Service Request |
| ListServ | All Agencies | Service Request |
| SAP Learning Solution –LSO | All Agencies | Automatically |
| SharePoint Online | All Agencies | Service Request |
| SharePoint 2013 On-Premises Shared Service | All Agencies | Service Request  |
| Virtual Desktop Services | All Agencies | Service Request |
| VMware Licensing – Resident Consultant Service | All Agencies | Service Request |
| Voice & Unified Communications Division (V/UCD) for Enterprise Call Center Services (ECCS) – Genesys  | All Agencies | Service Request |
| Voice & Unified Communications Division (V/UCD) for Enterprise Cisco WebEx Platforms | All Agencies | Service Request |
| Voice & Unified Communications Division (V/UCD) for Enterprise Mobile Management Service (EMMS) – AirWatch  | All Agencies | Automatically |
| Voice & Unified Communications Division (V/UCD) for Enterprise Verizon/Unify Platforms | All Agencies | Service Request  |
| Web Map Hosting | All Agencies | Service Request |
| **Professional Services** |
| Cloud Use Case Review | All Agencies | Service Request |
| Desktop Support | Consolidated Agencies Only | Automatically |
| EARC Intake Form | All Agencies | Service Request |
| Enterprise IT Policy Management | All Agencies | Service Request |
| LAN Support | Consolidated Agencies Only | Automatically |
| Voice & Unified Communications for Consolidated Agencies | Consolidated Agencies Only | Service Request |
| Web Site or Content Development and Support | All Agencies | Service Request |
| **Security Services** |
| Advanced Persistent Threat (APT) Protection | All Agencies | Automatically |
| Application Source Code Scanning Utilizing IBM Rational Appscan | All Agencies | Service Request |
| Cloud Access Portal (ITP-SEC003 Waiver) | All Agencies | Service Request |
| Commonwealth User Provisioning and Self-Service (CUPSS) | All Agencies | Automatically |
| Computer Forensics Investigations | All Agencies | Service Request |
| COPA Identity Exchange | All Agencies | Service Request |
| Cyber Security Training & Awareness | All Agencies | Automatically |
| eDiscovery and Forensics | All Agencies | Service Request |
| Enterprise Directory Services | All Agencies | Service Request |
| Endpoint Protection | All Agencies | Automatically |
| Incident Response and Investigations | All Agencies | Service Request |
| Information Security Officer – ISO | All Agencies | Service Request |
| Information Technology Governance, Risk, and Compliance (IT-GRC) Solution | All Agencies | Service Request |
| Internet Access Compliance and Control Management | All Agencies | Automatically |
| Perimeter Threat Protection | All Agencies | Service Request |
| Risk-Based Multi-Factor Authentication (RBMFA) | All Agencies | Service Request |
| Security Assessment | All Agencies | Service Request |
| Single Signon | All Agencies | Service Request |
| Social Engineering Security Awareness Training | All Agencies | Service Request |
| Vulnerability Management | All Agencies | Service Request |
| Vulnerability Scanning | All Agencies | Service Request |
| Web Application Firewall | All Agencies | Service Request |
| Web Application Vulnerability Scanning | All Agencies | Service Request |
| Web Content Reporting | All Agencies | Automatically |
| **Software as a Service (SaaS)** |
| Address Verification | All Agencies | Service Request |
| Alerting and Notifications | All Agencies | Service Request |
| Application Development & Support | Both | Service Request |
| ArcGIS Desktop Tools | Both | Service Request |
| Daptiv Project Portfolio Management | All Agencies | Service Request |
| Geocoding | All Agencies | Service Request |
| GIS Data Hosting and Metadata | All Agencies | Service Request |
| IES ERP Business Application Services | All Agencies | Service Request |
| Information Technology Service Management (ITSM) System | All Agencies | Service Request |
| OneDrive for Business (OD4B) | All Agencies | Service Request |
| PA Map Gallery | All Agencies | Service Request |
| TomTom Tools | All Agencies | Service Request |
| Web Map Creation | All Agencies | Service Request |

Infrastructure as a Service  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **EDC Services**

Service Description

Service Offerings provided by the Office of Administration, Office for Information Technology, Enterprise Data Center (EDC).

What is Included

* Additional Memory for Virtual Server
* Additional Memory for Virtual SQL Server
* Additional vCPU for Virtual Server
* Additional vCPU for Virtual SQL Server
* ADFS Services
* Backup Capacity 30 Day Retention (Disk)
* Backup Capacity Archive Retention (Tape)
* Datacenter Smart Hand Support
* Microsoft SQL DataBase Hosting & Support Shared Infrastructure
* Microsoft SQL DB Deployment on Shared Infrastructure with AlwaysOn Configuration
* Microsoft SQL DB Deployment per Database on Shared Infrastructure
* Microsoft SQL DB Server Build per Server
* Network Connectivity per Port
* Physical Server Operational Support
* Proxy Services Infrastructure and Support (per Application / per Environment)
* SAN Connectivity per Port
* SiteMinder Services (per Application / per Environment)
* SSL Certificate
* Standard Implementation Services per Physical Server
* Standard Implementation Services per Virtual Server
* Standard Production SSL Certificate
* Standard Virtual Dedicated Stand-Alone SQL Server
* Standard Virtual Windows 2012 R2 Server
* Storage – Tier 0 SAN per GB
* Storage – Tier 1 SAN per GB
* Storage – Tier 2 SAN per GB
* Virtual Server Operational Support

Service Levels

Availability Service Level Objective:

* Target 99% uptime.

Service Activation Service Level Objective:

* Standard Service Deployment is 1 – 2 weeks upon acceptance of the Solution Proposal.

Response Time Service Level Objective:

* **Urgent** – Critical Production Application is down or Service unavailable – Immediate.
* **High** – Connectivity issues or Performance issues – 1 business day.
* **Medium** – Request for service or Request for deployment – 2 to 5 business days.
* **Low** – Questions or Informational request – 6 to 10 business days.

Additional Information

Enterprise Data Center reference documents which provides more in-depth details of this service are available at

<https://itcentral.pa.gov/TechServ/Pages/EDC.aspx>

Infrastructure as a Service 

## **EDC Services: Service Request Status**

Service Description

ServiceNow is currently a pass-thru for EDC Services, therefore request status for these services are not available in ServiceNow. Users can request status of these items through this item.

What is Included

N/A

Service Levels

N/A

Additional Information

N/A

Platform as a Service 

## **Campus Wireless**

Service Description

Wireless access to the user’s agency network, agency network resources, and internet when visiting commonwealth locations participating with Campus Wireless.

Agency user works with local agency helpdesk for wireless access. Local agency IT staff works with Enterprise Network Services for initial setup.

What is Included

This service will provide agency users with wireless access to their network from other commonwealth locations participating with campus wireless.

Service Levels

None

Additional Information

ENS provides documentation when agency engages for this service via a ServiceNow request.

Enterprise Network Services / Wireless / Anchor/Mobility Management

Platform as a Service 

## **Enterprise Business Intelligence Suite (Business Objects)**

Service Description

Shared Service Offering provides all agencies with a business intelligence application to create reports and dashboards by bringing together data from multiple systems.

What is Included

* Provides software licenses for both Centralized Business Objects Enterprise and De-centralized BOE.
* Provides a fully-managed Centralized Business Objects Enterprise server environment with software version controls, capacity planning, and backups.
* Administers folders, user’s permissions and firewalls.
* Maintains Business Objects developer’s portal and intranet.
* Enables development of both reports and dashboards from defined “universe of data”.

Optional features of this service are:

* Development by Integrated Enterprise System (IES) of a “universe of data” built from agency specific SAP data.
* Assist in agency development of reports and/or dashboards using the agency specific “SAP universe of data”.
* Development by OA of a “universe of data” built from agency specific data but does not include SAP data.
* Assist in agency development of reports and/or dashboards using the agency specific “OA universe of data”.

Service Levels

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

Contact RA-businessobjects@pa.gov for additional information about this service.

The components that make up the EQRA package (Enterprise Query, Reporting, and Analysis) are the following:

* Business Objects Enterprise Premium.
* Business Objects Xcelsius Enterprise Interactive Viewing.
* Business Objects Live Office
* Xcelsius Enterprise.
* Crystal Reports – Desktop Developer.
* Publisher.
* Web Intelligence/Rich Client.
* Business Objects Voyage.

Platform as a Service 

## **Enterprise Messaging**

Service Description

Provides a consistent, reliable, and secure platform for communication, collaboration and desktop/laptop computing for commonwealth agencies under the Governor’s jurisdiction. Common services include Active Directory, MS Exchange, and Message Hygiene.

What is Included

* Active Directory integration
* Microsoft Exchange (email)
* Outlook Web Access
* Email encryption
* Anti-spam

Service Levels

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

Enterprise Messaging reference documents which provides more in-depth details of this service are available at <https://itcentral.pa.gov/TechServ/Pages/Messaging.aspx>

Platform as a Service 

## **Global Managed File Transfer (MFT)**

Service Description

The MFT service facilitates secure transfer of electronic files across customers and their stakeholders, and provides the configuration of automated workflow capabilities to support business processes. The service is used to securely transfer files that are too large to be sent via email and/or accessible from a commonwealth website.

What is Included

* Support multiple file transfer protocols including FTP/S, SFTP and HTTP/S.
* Securely transfer files over public and private networks using. encrypted file transfer protocols.
* Capable of Securely storing files using data encryption methods.
* Automate file transfer processes between Agencies and business partners including detection and handling of failed file transfers using an integrated workflow engine.
* Generate detailed reports on user and file transfer activity.

Service Levels

Priority Levels and Allowable Response Times

* + - 1. Critical– within 30 minutes to respond to customer
			2. High– up to 8 hours to respond to customer
			3. Medium– up to 24 hours to respond to customer
			4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime

Additional Information

None

Platform as a Service 

## **Kofax Enterprise E-Fax**

Service Description

Kofax E-Fax allows customers to send/receive faxes electronically from email clients, desktop computers or hosted applications.

What is Included

* Send faxes through email (Supports file attachments)
* Receive faxes through email as tiff or pdf attachments
* Send faxes from SAP
* Send/Receive faxes from web based applications
* Send/Receive Faxes from File Servers

Service Levels

Priority Levels and Allowable Response Times

* + - 1. Critical– within 30 minutes to respond to customer
			2. High– up to 8 hours to respond to customer
			3. Medium– up to 24 hours to respond to customer
			4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

None

Platform as a Service 

## **ListServ**

Service Description

ListServ is used to target a specific audience, greater than 1,000 recipients, with one-way communications. Agencies may have multiple distribution lists within ListServ, and those distribution lists target recipients. Each distribution list contains approval authority/owner association, which names individuals within the agency who have approval authority for distributing the communications and maintaining the distribution list(s). The owner of the distribution list has the ability to enter any email address internal or external to the Commonwealth into their respective distribution list(s).

What is Included

* Newsletter Templates
* Template Gallery
* Newsletter Testing: The newsletter testing feature allows users to send test messages to their own addresses before posting. This is particularly useful for HTML newsletters since HTML standards support can vary widely across different email clients.
* HTML Mail Templates: List owners can choose to have confirmation and informational messages sent out in HTML. A number of pre-designed HTML mail template styles are available. List owners can also easily create their own HTML mail template styles for their lists.
* Message Scheduling: The message scheduling option allows senders to schedule the delivery of their newsletters and announcements at a specific time and date, without having to be present at the time of delivery.
* CSV Reports: List, subscriber and server usage reports can now be downloaded as CSV files and exported to Excel or other external applications.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

None

Platform as a Service 

## **SAP Learning Solution – LSO**

Service Description

The SAP Learning Solution – LSO is a comprehensive learning management system.

What is Included

Standard SAP Learning Solution – LSO functionality – Agency and enterprise training catalogs, search capability, course registration, curriculum management, participation management, reporting, transcripts, web based training delivery, on-line evaluations, on-line tests, and multiple administrator roles.

Service Levels

None

Additional Information

To request hands on training contact - ra-lsoadministrator@pa.gov

Use the following links to download procedural desk references:
[Learners](http://eniesrwda01.state.pa.us/gm/folder-1.11.85500) –  [Supervisors](http://eniesrwda01.state.pa.us/gm/folder-1.11.85499) – [Instructors](http://eniesrwda01.state.pa.us/gm/folder-1.11.85502) -  [Reporters](http://eniesrwda01.state.pa.us/gm/folder-1.11.85501) [Administrators](http://eniesrwda01.state.pa.us/gm/folder-1.11.85660)

 Learner, supervisor and reporter Web based training can be found in the SAP Learning Solution – LSO catalog at, OA sponsored trainings for all agencies.

Platform as a Service 

## **SharePoint Online**

##

Service Description

SharePoint Online is a cloud-based service that helps organizations share and collaborate with colleagues, partners, and customers. With SharePoint Online, you can access internal sites, documents, and other information from anywhere – at the office, at home, or from a mobile device.

What is Included

* Sites – Allows for the creation of customized sub-sites under a given SharePoint site. Sites may be targeted to a particular department of an organization or a particular user group or subject matter.
* Communities – Allows users to share knowledge and information with each other and may involve activities such as: information sharing, knowledge sharing, content tagging, user feedback and more.
* Content – SharePoint Online is a collection of web-based tools and technologies that help store, share, and manage digital information. The hosted service is ideal for working on projects, storing data and documents in a central location, and sharing information with others.
* Search – Allows users to search for content, documents, images or people within a SharePoint site with a power search engine.
* Insights – Enables native integration with other Microsoft products and services such as: Excel Services, Visio, PowerPivot, SQL Server and Reporting services.
* Composites – Enables the development of customized solutions by integrating existing pieces of applications developed separately. These may be external software or external data connectivity.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

To request a site, or for information and documentation regarding the shared service is available at [SP Central](http://spcentral.oa.pa.gov/).

Platform as a Service 

## **SharePoint 2013 On-Premises Shared Service**

Service Description

This enterprise service will support Standard and Enterprise versions of SharePoint.

What is Included

Sites – Allows for the creation of
Service Features are based on the version of SharePoint agencies are interested in leveraging. Agencies are responsible for procuring the necessary end user Client Access Licenses that are needed to leverage the service & will need to provide copies of Client Access License Purchase Orders to the Office for Information Technology.

Standard Features:

* Intranet and Extranet Service.
* Internet secured access to SharePoint for authenticated users (CWOPA, USER, MUSER domains).
* SharePoint Production, Staging and Development environments.
* Service platform (hardware/software) life cycle management (i.e., capacity, upgrades, patches, etc.).
* Support for troubleshooting infrastructure, security, and site collection administration issues.
* Tier 2 and Tier 3 SharePoint help desk support during normal business hours (8am to 5pm) Monday thru Friday.
* 24x7 infrastructure support with scheduled maintenance.
* Infrastructure recovery within 24 hours.
* Daily database backups.
* Change Advisory Board consisting of the Bureau of Application Management Services, Enterprise Technology Services Office, and agency site collection administrators.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

To request a site, or for information and documentation regarding the shared service is available at [SP Central](http://spcentral.oa.pa.gov/).

Platform as a Service 

## **Virtual Desktop Services**

Service Description

This Service delivers a virtualized Windows Desktop that resides in the data center that can be accessed by an end user device from within the COPA network or remote. Operating systems that are supported for connecting to the virtual desktops include Microsoft Windows, Apple Macintosh OSX, Apple IOS (iPad/iPhone), and Android.

What is Included

* Setup of environment for Agency IT staff to build, deploy, and manage a custom desktop image for deployment to agency end users.
* Guidance for recommended configurations based on use cases for targeted users.
* Administrator training for administering the desktops from a deployment and operational support perspective.
* Documentation for a standard user deployment and configuration of end user devices for connecting to their assigned virtual desktops.
* Tier2 support for agency administrators for troubleshooting and deployment assistance.

Service Levels

Describes the level of service expected between the service provider and customer, documenting service level targets and the responsibilities of the service provider and the customer. This can include contractual Service Level Agreements, non-contractual Service Level Objectives or Operational Level Agreements.

Additional Information

A start-up and deployment guide will be provided to all agency VDI administrators to assist with implementing and deploying their virtual desktops.

Sample end user training (documentation and videos) will also be provided that the agency can use.

Platform as a Service 

## **VMware Licensing – Resident Consultant Service**

Service Description

OA offers VMware Licensing and Resident Consultant Services available through the COPA-VMware Enterprise License Agreement (ELA).

What is Included

This can include licensing costs, subscription and support or on location Resident Consultant Services and Training.

Service Levels

None

Additional Information

None

Platform as a Service 

## **Voice & Unified Communications Division (V/UCD) for Enterprise Call Center Services (ECCS) - Genesys**

Service Description

Delivers SME support of Voice Services ECCS - Genesys

This also extends to agencies not under the Governor’s Jurisdiction with regards to the Telecommunications Contract. Those agencies are not required to use the Telecommunications Contract but can utilize it at any time, in which case the V/UCD assists and guides them to the services they need.

What is Included

* Assist with design and configuration of new services
* Provides maintenance patching via Vendor maintenance schedules
* Provides assistance to agencies are not receiving prompt service from contracted vendors
* Provide guidance on upgrades to the platform
* Informs enterprise agencies of multi-agency outage via Incident Reports (IR)

Note: Devices that are not purchased/owned by the Commonwealth are not supported.

Service Levels

• Request for guidance on Move/Add/Changes = SLO assigned between V/UCD and agency, based on agencies needs depending on scope of the project

• Design/Implementation of a New System = SLO assigned between V/UCD and agency, based on agencies needs depending on scope of the project

• Request for outage escalation = See response times below

Response Time:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes
* **High** – Non-business-critical process impacting multiple people - 1 hour
* **Medium** – Request for service - 8 hours
* **Low** - Questions or informational requests - 16 hours

Additional Information

Genesys

Platform as a Service 

## **Voice & Unified Communications Division (V/UCD) for Enterprise Cisco WebEx Platforms**

Service Description

Delivers SME and ordering support of Enterprise Cisco WebEx platforms.

This also extends to agencies not under the Governor’s Jurisdiction with regards to the Telecommunications Contract. Those agencies are not required to use the Telecommunications Contract but can utilize it at any time, in which case the V/UCD assists and guides them to the services they need.

What is Included

* Informs enterprise agencies of outages via Incident Reports (IR)
* Provides assistance to agencies are not receiving prompt service from contracted vendors
* Provides maintenance patching via Vendor maintenance schedules

Service Levels

* Request for ordering licenses = 1-day SLA
* Request for outage escalation = See response times below
* SLO assigned between V/UCD and agency, based on agencies needs depending on scope of the project

Response Time:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes
* **High** – Non-business-critical process impacting multiple people - 1 hour
* **Medium** – Request for service - 8 hours
* **Low** - Questions or informational requests - 16 hours

Additional Information

None

Platform as a Service 

## **Voice & Unified Communications Division (V/UCD) for Enterprise Mobile Management Services (EMMS) - AirWatch**

Service Description

Delivers enterprise mobile device managed platform as a service as well as subject matter expert support of Voice Services EMMS - AirWatch
This also extends to agencies not under the Governor’s Jurisdiction with regards to the Telecommunications Contract. Those agencies are not required to use the Telecommunications Contract but can utilize it at any time, in which case the V/UCD assists and guides them to the services they need.

What is Included

* Assists with design and configuration of new AirWatch services
* Provides maintenance patching via Vendor maintenance schedules
* Provides assistance to agencies that are not receiving prompt service from contracted vendors
* Provides guidance on upgrades to the platform
* Educates customer agencies about service capabilities, forthcoming features, and platform changes via the TMO user group.
* Informs enterprise agencies of multi-agency outage, and service interruption via Incident Reports (IR)

Note: Hardware devices that are not purchased/owned by the commonwealth are not supported beyond the Bring Your Own Device (BYOD) environment.

Service Levels

Request for guidance on Add/Changes = No non-contractual SLO assigned, based on agencies needs

Request for outage escalation = See response times below

Response Time:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes
* **High** – Non-business-critical process impacting multiple people - 1 hour
* **Medium** – Request for service - 8 hours
* **Low** - Questions or informational requests - 16 hours

Additional Information

<http://www.air-watch.com/resources/>

Platform as a Service 

## **Voice & Unified Communications Division (V/UCD) for Enterprise Verizon/Unify Platforms**

Service Description

Delivers voice ESMS products as a service as well as subject matter expert support of Voice Services such as the VoIP PennConnect platform, Unified Communications (UC), and analog phone systems. This also includes Verizon Contact Center (VCC) an enterprise call center solution, OpenScape Contact Center (OSCC) a proprietary VoIP call center solution based upon the PennConnect platform, Toll-Free (TF) and Pay Phone support.

This also extends to agencies not under the Governor’s Jurisdiction with regards to the Telecommunications Contract. Those agencies are not required to use the Telecommunications Contract but can utilize it at any time, in which case the V/UCD assists and guides them to the services they need.

What is Included

* Assists with design and configuration of new services
* Provides maintenance patching via Vendor maintenance schedules
* Provides assistance to agencies that are not receiving prompt service from contracted vendors
* Provides guidance on upgrades to the platform
* Educates customer agencies about service capabilities, forthcoming features, and platform changes via the TMO user group.
* Informs enterprise agencies of multi-agency outage, and service interruption via Incident Reports (IR)

Note: Devices that are not purchased/owned by the Commonwealth are not supported.

Service Levels

* Request for guidance on Move/Add/Changes = No non-contractual SLO assigned, based on agencies needs
* Design/Implementation of a New System = No non-contractual SLO assigned, based on agencies needs
* Request for outage escalation = See response times below

Response Time:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes
* **High** – Non-business-critical process impacting multiple people - 1 hour
* **Medium** – Request for service - 8 hours
* **Low** - Questions or informational requests - 16 hours

Additional Information

ESMS for full catalog of services: <https://esms.pa.gov/>

-IPT training material: <http://www.oa.pa.gov/Programs/Information%20Technology/Pages/Penn-Connect-Unified-Communications.aspx#.V1rVlKPD__I>

-The TMO SharePoint site for service news and upcoming TMO events as well as support material: <https://etso.oa.pa.gov/ComputeTransition/SitePages/Home.aspx>

-Verizon PennConnect trainer: Contact the VCSD at 877.302.7366

Platform as a Service 

## **Web Map Hosting**

Service Description

Delivers use of hardware and geospatial software that is required to place a web map and/or web map application on the Internet/Intranet.

What is Included

* Offers shared service for use by multiple agencies.
* Uses commonwealth standard tool set of ArcGIS Server software.
* Provides a testing and robust staging and production infrastructure.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

 None

Professional Services 

## **Cloud Use Case Review**

Service Description

Provides a framework that can be utilized to assess what impact the Cloud Use Case may have on the enterprise as it pertains to network, security, legal and financial.

This review does not replace existing processes such as COPPAR and CA2.

What is Included

Guidance to understand the impact to the commonwealth

Service Levels

None at this time

Additional Information

A confirmation email will be provided upon submittal. The Cloud Services Team will respond with additional questions as required in order to determine approval or denial of the Use Case

Professional Services 

## **Desktop Support**

Service Description

Delivers support of employee personal computing hardware and software systems.

What is Included

* Setup for new employees and contractors.
* Obtain quote of hardware and software for Agency purchase.
* Installation and configuration of equipment including laptop, workstation, printer, and peripheral devices.
* Installation and configuration of software which run on the desktop.
* Provides scheduled software maintenance patching.
* Troubleshooting of hardware and software.
* Upgrade, replacement and disposal of all desktop equipment.
* Asset management of desktop equipment and software.

Service Levels

Installation and Configuration Completion Service Level Objective:

* Target: Schedule/respond within 5 business days of the request.
* Target: Completion is within 20 days.
* Large scale installations are exempt.

Resolve Time Service Level Objective:

* Target: 60% of all reported Break/Fix issues resolved within 1 business day.

Response Time Service Level Objective:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes.
* **High** – Non-business-critical process impacting multiple people – 1 hour.
* **Medium** – Request for service – 8 hours.
* **Low** – Questions or informational requests – 16 hours.

Additional Information

None

Professional Services 

## **EARC Intake Form**

Service Description

Service Levels

N/A

Additional Information

Enterprise Architecture Review Committee Intake Form – Redirect to vRealize. This form captures basic information regarding a new service item request to be brought before the Enterprise Architecture Review Committee for consideration. The VMWare vRealize / vOrchestration is the system of record (SoR) for intake of the end user/agency requests. The datastore entails additional business rules and tracking.

What is Included

This form captures basic information regarding a new service item request to be brought before the Enterprise Architecture Review Committee for consideration.

End users for the system that require additional assistance should contact via email is RA-OAEARC@pa.gov All information, training material and standard procedures may be found on the EARC portal.

Professional Services 

## **Enterprise IT Policy Management**

Service Description

Provide lifecycle management support for OA-OIT IT policies (e.g., creation, revisions, rescission, and publication).

What is Included

* Requests for the creation of new IT policies
* Requests for revisions to existing IT Policies
* Requests for IT policy research and assessments

Service Levels

SLO: Expedited Policy Revisions: 10-working day turnaround (at direction of the Commonwealth CIO or CISO)

SLO: Emergency Policy Revisions: 5-working day turnaround (at direction of the Commonwealth CIO or CISO)

SLO: Normal Policy Revisions: 65 working days (from request approval to final publication)

Additional Information

Reference site for all current IT Policy publications and IT Policy Lifecycle Management procedural document are available on IT Central. <https://itcentral.pa.gov/Pages/IT-Policies.aspx>

Professional Services 

## **LAN Support**

Service Description

Delivers configuration, setup and on-going maintenance of Local Area Network (LAN) to provide connectivity for local computing and printing resources within a building or campus environment.

Note: This service is only available to the consolidated agencies.

What is Included

* Network administration to include Local Area Network switches, firewalls, routers, Internet content filters, and Dynamic Host Configuration Protocol services.
* Server administration to include installation and configuration of server hardware and software in support of all File and Print functions and network infrastructure.

System administration to include patching, software packaging and distribution, and system configuration reporting.

Note: This service is only available to the Office of Administration and the consolidated agencies:

* Budget
* Emergency Management
* General Counsel
* General Services
* Governor’s Office
* Historical and Museum Commission
* Human Relations Commission
* State Police
* State
* State Tax Equalization Board

Service Levels

Availability Service Level Objective:

* Target: 99.5% uptime during business hours of 7:30 AM to 5:00 PM.

Response Time Service Level Objective:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes.
* **High** – Non-business-critical process impacting multiple people – 1 hour.
* **Medium** – Request for service – 8 hours.
* **Low** – Questions or informational requests – 16 hours.

Additional Information

None

Professional Services 

## **Voice & Unified Communications for Consolidated Agencies**

Service Description

Delivers support of employee desktop VoIP, Unified Communications (UC), and analog phone systems. This also includes wireless smartphones, cell phones and MiFi hot spots with Mobile Device Management (MDM) support.

Note: This service is only available to the Office of Administration and the consolidated agencies.

What is Included

* Setup for new employees and contractors
* Obtain quote of hardware for Agency purchase
* Installation and configuration of equipment including VoIP and analog phone sets, UC on the desktop and wireless devices
* Provides maintenance patching via Vendor maintenance schedules
* Troubleshooting of hardware and software
* Upgrade, replacement and disposal of all equipment
* Asset management of desktop equipment
* Other Vendor provided services include Virtual Call Center design/activation and Toll-Free services

Note: Devices that are not purchased/owned by the Commonwealth are not supported.

Service Levels

* Repair Calls; Password resets = 1 Day resolution
* Repair Calls = 2 business days (No Vendor SLA available)
* Request for Move/Add/Changes = 10-15 days (No Vendor SLA available)
* Design/Implementation of a New System or new IPT line = 30 business days after approval of design
* Request for New/Replacement Wireless = 9 business days (No Vendor SLA available and each wireless vendor has different processing times)

Response Time:

* **Urgent** – Business-critical production outage impacting multiple people – 15 minutes
* **High** – Non-business-critical process impacting multiple people - 1 hour
* **Medium** – Request for service - 8 hours
* **Low** - Questions or informational requests - 16 hours

Additional Information

None

Professional Services 

## **Web Site or Content Development and Support**

Service Description

Delivers web site maintenance and support solutions that meet specific customer requirements.

Note: This service is only available to the consolidated agencies.

What is Included

* Provide web site conversion options.
* Ensure adequate portal security measures are followed.
* Provide documentation options.
* Provides a process for updating, maintaining and modifying an existing supported web site.
* Work with business analyst, project manager or end user to gather requirements.
* Provide system coding as needed.
* Ensure commonwealth standards are followed.
* Plan and coordinate web site modifications with the business owner.

Service Levels

Agreed upon uptime between the business owner and development team.

Additional Information

None

Security Services 

## **Advanced Persistent Threat (APT) Protection**

Service Description

Advanced Persistent Threat (APT) is a solution to identify and block zero-day web exploits, binaries and multi-protocol callbacks to help CoPA scale their advanced threat defenses. The selected APT solution set includes network visibility fabric, deep session inspection and SSL decryption as well as forensic integration and packet capture technologies. The solution also includes an endpoint software that is deployed to approximately 80,000 servers and desktops. Verizon is a key service provider since a majority of the solution is deployed at their colocation space in Pittsburgh and managed network egress points in Harrisburg.

What is Included

The solution generates alerts that EISO sends to agencies as security incidents they are required to remediate. In most cases, triage activities such as blocking the IP address or URL that triggered the alert is requested by EISO and implemented by ETSO.

Service Levels

None

Additional Information

Additional information about APT can be found at <https://itcentral.pa.gov/Security/Pages/default.aspx>

Security Services 

## **Application Source Code Scanning Utilizing IBM Rational Appscan**

Service Description

Application code is scanned as it is being developed to reveal security vulnerabilities and errors before code is released in a production environment.

What is Included

Application Source Code Scanning

Service Levels

Priority Levels and Allowable Response Times:

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

Reference documents which provides more in-depth details of this service are available at www.cybersecurity.state.pa.us

Security Services 

## **Cloud Access Portal (ITP-SEC003 Waiver)**

Service Description

Cloud Management Portal access. Required per ITP-SEC003.

Enterprise level AD Group has been created to control Cloud Portal Access to sites that offer the ability to manage and develop off-premise based application development & hosting services. Agency level AD Groups will no longer be valid.

What is Included

The Enterprise Level AD Group will contain all Agency users that need to access their Cloud site for management and application development only.

Service Levels

None

Additional Information

None

Security Services 

## **Commonwealth User Provisioning and Self-Service (CUPSS)**

Service Description

Automated management of users in the CWOPA domain and Microsoft Exchange based on HR activity – mandatory service for all agencies, etc. under the Governor’s jurisdiction.

What is Included

* Automated account creation, separation, other changes based on HR activity, some manual operations (including group management, account suspension, resets), self-service password changes or reset of forgotten password.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us).

[CUPSS FAQ v1-1](https://collab.pa.gov/oa/EISO/Shared%20Documents/Identity%20and%20Access%20Management/CUPSS%20FAQ%20v1-1.docx)

Security Services 

## **Computer Forensics Investigations**

Service Description

Service Offerings provided by the Office of Administration, Office for Information Technology, Enterprise Technology Services Office (ETSO).

What is Included

* Provides systematic inspection of commonwealth systems and their contents for evidence or supportive evidence of cybercrimes or another computer use that is being inspected.
* Collects and analyzes evidence in a fashion that adheres to standards of evidence that are admissible in a court of law.
* Identifies the cause of incident.
* Contains compromised service.
* Identifies policy violation.
* Recommends appropriate repair of discovered vulnerabilities.
* Performs scanning and evaluation after repair of device.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us).

Security Services 

## **COPA Identity Exchange**

Service Description

NSTIC Identity Exchange registers users in the citizens’ directory (SRPROD) and provides optional verification of their identity through PennDOT or a third party. It also enables single-signon with SAML and Shibolith.

What is Included

Citizen registration and management, optional identity verification, and SAML/ Shibolith plugin for single signon.

Service Levels

None

Additional Information

[Relying Party Technical Specifications](https://collab.pa.gov/oa/EISO/Shared%20Documents/Identity%20and%20Access%20Management/Relying%20Party%20Technical%20Specification.pdf)

[SAML Flow](https://collab.pa.gov/oa/EISO/Shared%20Documents/Identity%20and%20Access%20Management/Phase1_saml_flow.pdf)

Security Services 

## **Cyber Security Training & Awareness**

Service Description

A preventive security measure that includes Social engineering testing through end user email phishing campaigns that can be conducted as a means of identifying staff vulnerability to similar phishing schemes and address it through additional training. This service also includes Annual Cyber Security

Awareness Training for all employees.

What is Included

* Vulnerability validation
* Phishing simulations (Social Engineering)
* Annual Cyber Security Awareness training (as required by MD 205.34)

Service Levels

There are no SLA’s or OLA’s associated with these services.

Additional Information

Reference documents which provides more in-depth details of this service are available at www.cybersecurity.state.pa.us

Security Services 

## **eDiscovery and Forensics**

##

Service Description

Conducting an investigation of electronic data such as email, instant messages, internet history, word processing files, spreadsheets, social networking content that is stored on desktops, laptops, file servers, mainframes, smartphones, and employees’ home computers or on a variety of other platforms.

What is Included

Customers will receive a forensically sound copy of all electronic data pertinent to the investigation request (may also include a forensic report depending upon the type of material found). Additional information can be requested by a customer on a case by case basis.

Service Levels

None

Additional Information

Additional information about eDiscovery can be found at

<https://itcentral.pa.gov/Security/Pages/default.aspx>

Security Services 

## **Endpoint Protection**

Service Description

Monitoring desktops and servers for security issues.

What is Included

**Endpoint DLP**

Endpoint DLP is a data loss prevention tool consisting of endpoint protection, network monitoring and data at rest protection – to help prevent data loss. The Commonwealth will use the DLP solution to identify, monitor and protect sensitive and confidential Citizen PII in use, data in motion, and data at rest through deep content inspection and analysis of information exchange. This overall DLP solution monitors the usage, access, transfer, sharing and storage of citizen PII within the Commonwealth’s infrastructure of more than 80,000 users. The DLP solution helps detect and prevent the unauthorized use and transmission of sensitive and confidential Citizen PII. Endpoint DLP secures the endpoints where the data resides – whether in transit on the network, at rest in storage or in use by users. Not having this solution greatly increases the chances of breach due to internal misuse or intentional or non-intentional insider threat.

**Endpoint Drive Encryption**

McAfee Endpoint Drive Encryption, also referred to as full disk encryption, is encryption software that helps protect data on Microsoft Windows tablets, laptops, desktop PCs, and workstations to prevent the loss of sensitive data, especially from lost or stolen equipment. Drive encryption is designed to make all data on the system drive unintelligible to unauthorized persons, which in turn helps meet compliance requirements. Not having this tool would lead to data breaches if and when laptops or portable computers and devices were lost or stolen.

**Host Intrusion Prevention System (HIPS)**

McAfee Host Intrusion Prevention System (HIPS) monitors a single host for suspicious activity by analyzing events occurring within that host. HIPS solutions protect the host from the network layer all the way up to the application layer against known and unknown malicious attacks. In case of attempted operating system or application changes by a hacker or malware, HIPS blocks the action and alerts the user so an appropriate decision on next steps can be made.

**Enterprise Antivirus**

Antivirus software is used to safeguard a computer from malware, including viruses, computer worms, and trojans. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious software. McAfee Enterprise Antivirus provides for endpoint protection for workstations and servers. Not having basic Antivirus protection in place will have a far reaching and quite severe negative impact on the security posture of the commonwealth and will lead to hundreds if not thousands of infected machines - because there would be no Antivirus to protect it from infection. Among those Infections - such as keyloggers - would capture each users “keystrokes” as they type away across the keyboard. No antivirus on the machine to stop it would send the keystrokes to distant lands. Commonwealth data in the hands of hackers. That would certainly lead to a large # of data breaches which the commonwealth could not afford to have - both financially, as well as the damage there events would undoubtedly cause to the commonwealth's reputation.

**Advance Persistent Threat Agent**

The Endpoint Agent, also referred to as the "HX Agent", protects your networks by monitoring each endpoint device or host, collecting real-time data of events occurring on the endpoint, and identifying threat activity and evidence on the host that routinely bypass signature-based and defense-in-depth security systems (i.e. APT and Zero Day attacks).

Threat activity and evidence include:

- Unauthorized use of valid accounts
- Trace evidence and partial files
- Command and control activity
- Known and unknown malware
- Suspicious network traffic
- Valid programs used for malicious purposes
- Unauthorized file access

Adaptive security requires monitoring of all threat vectors, including fast, accurate assessments of potential cyber attacks tracked to endpoint activity. The Endpoint Agent allows you to detect, analyze, and respond to targeted cyber attacks and zero-day exploits on the endpoint.

When the agent finds evidence of potential compromises, it reports this information to the HX & HXD Series appliance. It also retrieves information and tasks (jobs) from the HX & HXD Series appliance and performs them. Tasks include upgrading indicators, requests for forensic information (file, triage, and data requests), and requests to contain the host machine.

Service Levels

None

Additional Information

Additional information about Endpoint Protection can be found at <https://itcentral.pa.gov/TechServ/Pages/default.aspx>

or [https://itcentral.pa.gov/Security/Pages/default.aspx](https://itcentral.pa.gov/TechServ/Pages/default.aspx)

Security Services 

## **Enterprise Directory Services**

Service Description

Enterprise Directory Services provide shared repositories of categorized users requiring common resource access such as employees/contractors (CWOPA), business partners (Managed Users), and citizens (SRPROD).

What is Included

* Active Directory repository management
* Active Directory user administration (add, remove, update, etc.)
* Self-service capabilities (e.g. password reset)
* Virtual Directory services

Service Levels

None

Additional Information

[Enterprise Access Services](https://itcentral.pa.gov/sites/Enterprise_Access_Services/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FEnterprise%5FAccess%5FServices%2FShared%20Documents%2F5%2E%20Supporting%20Documentation%2FDHS%2DDLI%2DDOT%20Documentation&FolderCTID=0x01200044E945504BA4BC4493D6BD53456C080C&View=%7B7628D2FE%2DDF9F%2D43F0%2D8874%2DE6E87129EB3A%7D)

Security Services 

## **Incident Response and Investigations**

Service Description

This service delivers expertise with detection, containment, mitigation, forensic investigation and remediation of malware, misuse and other negative impact activities on Commonwealth IT assets.

What is Included

* Malware detection and removal
* Determination of misuse
* Forensic acquisitions from workstations and servers
* Chain of custody and attestation services
* Packet capture and data correlation Support

Service Levels

None

Additional Information

Additional information about Incident Response & Investigations can be found at <https://itcentral.pa.gov/Security/Pages/default.aspx>

OR

https://itcentral.pa.gov/Security/Pages/default.aspx

Security Services 

## **Information Security Officer - ISO**

Service Description

The ISO role is designed to be a conduit between an agency, the Commonwealth EISO office and security operations teams. An ISO can also be a primary element in creating / modifying an agency security program to meet security or audit requirements.

An MOU will be signed between OIT and the agency that is requesting this service.

What is Included

* Coordinate the implementation of detective, corrective or preventative information security measures as necessary and provide the EISO CISO assurance that the organization complies with legislative, contractual, regulatory and Commonwealth policy requirements regarding information security.
* Ensure appropriate organizational security procedures and standards are in place to support agency information security policy and regulatory requirements. These standards may be Commonwealth ITP related or third party contractual/legislative requirements.
* Act as an intermediary in between the agency and the OA EISO office, OA Security Operations teams, OA application teams and others to ensure technologies are implemented appropriately.

Determine the appropriate sensitivity for data and appropriate risk controls.

Service Levels

None

Additional Information

Reference documents which provide more in-depth details of this service are available at <http://www.cybersecurity.state.pa.us>

Security Services 

## **Information Technology Governance, Risk, and Compliance (IT-GRC) Solution**

##

Service Description

The IT GRC solution provided by OA/OIT EISO encompasses a cyber-security risk framework which will show an enterprise an organizational view of security and IT risk across the enterprise – agency. The solution can be accessed by IT and business executives to view enterprise and agency risk, risk scores, and risk mitigation strategies. The solution provides an avenue to tie cyber to business risk across all agencies, and provides compliance metrics and reporting to IT admins, IT leaders up to the Governor cabinet level. The solution can be used to:

* Implement a cost effective IT GRC solution.
* Assess IT risk across the enterprise.
* Show compliance maturity.
* Assist agencies with tracking & mitigating IT risks.
* Show an enterprise and agency level IT risk score to all stakeholders.

What is Included

The solution includes the following services and access to supporting toolkits:

* Risk baseline: Establish and monitor a baseline security risk posture using leading industry standard such as the National Institute of Standards and Technology (NIST), Cyber Security Framework (CSF), consistently across the Commonwealth enterprise. Risk baseline identifies presence of similar weaknesses across the enterprise, and provides a correlation of root causes.
* Regulatory compliance: Develop competency on Commonwealth and federal regulations to assist agencies to perform periodic audits and review for readiness.
* Establish and monitor an enterprise Plan of Action & Milestones (POA&M): This helps identify and establish collaboration of agencies to implement similar safeguards. POA&M will be continuously monitored for completion of milestones.
* Security policy exception management: Maintain and monitor agency and datacenter exceptions to Commonwealth’s established security policy and risk baseline/POA&M.
* Financial risk management: Support the Commonwealth’s comptroller team to use OA EISO risk management automation for financial/cost management.
* Vulnerability assessment and penetration testing: Perform periodic assessments on the Commonwealth’s IT assets.
* Security Incident Management: Provide an enterprise platform OA EISO and for agencies to report, track, monitor and document security incidents, at an agency level (internal review) and escalation to OA EISO.
* COOP Enablement: Support COOP team to leverage OA EISO risk management tool kits for automation of agency and enterprise COOP plan, reporting, periodic testing and monitoring of resiliency safeguards.
* Integration of Security Tools: The program will leverage the capabilities of the existing security tools in the Commonwealth enterprise for establishing a transparent, accelerated and effective risk management process that can be monitored at various organization levels – agency and enterprise by providing appropriate information/reports to technology and business stakeholders.

Service Levels

IT GRC Service will be available to agencies 24/7/365.

Additional Information

Additional information about eGRC can be found at <https://itcentral.pa.gov/Security/Pages/default.aspx>

Security Services 

## **Internet Access Compliance and Control Management**

Service Description

This service provides logging and inspecting of Commonwealth internet activity.

What is Included

Proxy Enterprise Policy Management:

* Enterprise Baseline compliance Policy on the Enterprise Proxy.
* Agency specific policies

Enterprise Proxy Internet activity reporting services:

* Provides Internet compliance reports from the Proxy Internet logs to authorized agency personnel.
* Inspection of SSL sessions for malicious content

Service Levels

None

Additional Information

Additional information about Web Content Management can be found at <https://itcentral.pa.gov/Security/Pages/default.aspx>

Security Services 

## **Perimeter Threat Protection**

Service Description

Perimeter Threat Protection is a solution to monitor network ingress and egress points on the managed network that the commonwealth uses to conduct its business electronically. The solution includes firewall and intrusion detection services. Verizon is a key service provider since a majority of the solution is deployed at their colocation space in Pittsburgh and managed network points in Harrisburg.

What is Included

The solution allows for monitoring of inbound and outbound network connections and for the ability of infrastructure management teams to use firewall rules and intrusion detection to allow or deny connections to the commonwealth hosts.

Service Levels

SLAs are in place between CoPA and Verizon.

Additional Information

Additional information about Perimeter Threat Protection can be found at <https://itcentral.pa.gov/TechServ/Pages/default.aspx>

Security Services 

## **Risk-Based Multi-Factor Authentication (RBMFA)**

Service Description

This service provides CWOPA users with an additional layer of protection for data stored in the cloud and for other applications such as the VPN or ESS where there may be a higher risk or consequence to unauthorized access to systems or data. Users may be prompted for additional authentication such as a PIN or response to security questions based the transaction being attempted.

What is Included

* Risk evaluation of the transaction or data being accessed
* Second factor for authentication:
	+ Software token installed on the device, locked by a PIN
* One Time Passcode (OTP) send via SMS text message to a smart phone.

Service Levels

Tier 1 & 2 support handled by the agency; Tier 3 by EDC with support from Computer Associates (product vendor). Contractual obligation with CA Support is 4 hours.

Additional Information

FAQ: <https://itcentral.pa.gov/Security/EISO%20Documentation/Risk%20Based%20MFA%20FAQ%20v2.docx>

Security Services 

## **Security Assessment**

Service Description

Delivers consulting services to analyze and assess an agency’s security posture.

What is Included

* Conducts interview, inspections, assessments and policy reviews.
* Identify, quantify, and prioritized vulnerabilities in a system and infrastructure.
* Assures compliance with key security, physical, device, network, human, and policy controls.
* Details discovered risks and provide risk mitigation options for remediation in a written report.
* Offers review and guidance on policy and procedure development.
* Performs annual extensive audits and quarterly full audits.
* Performs application and host based security scans in response to CA2 requests.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at www.cybersecurity.state.pa.us

Security Services 

## **Single Signon**

Service Description

Single Signon provides a user the ability to utilize the same user ID and password to access multiple services.

What is Included

Uses either Computer Associates Siteminder, Active Directory Federation Services (ADFS), or Security Assertion Markup Language (SAML) to access enterprise directories and provide user login services.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us).

[Siteminder Rules of Engagement](https://collab.pa.gov/oa/EISO/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Foa%2FEISO%2FShared%20Documents%2FIdentity%20and%20Access%20Management&FolderCTID=0x012000296560E60A8F074E8AE47DC82B196847&View=%7BA3834336%2DEFFE%2D42E1%2DA437%2D118E61E63E66%7Dhttps://collab.pa.gov/oa)

Security Services 

## **Social Engineering Security Awareness Training**

Service Description

Ensures that all commonwealth users are familiar with information technology security best practices and policies.

What is Included

* Establish requirements for the correct security posture of employees and contractors that access computer networks.
* Ensure requirements for state and federal regulations are included in training.
* Procure and customize training courses.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at www.cybersecurity.state.pa.us

Security Services 

## **Vulnerability Management**

Service Description

Delivers mechanisms to prevent and/or defend against cyber-attacks as well as reduce vulnerabilities.

What is Included

* Exam application or network to determine adequacy of security measures with vulnerability scans and testing.
* Deploy and maintain anti-virus software.
* Isolate and remediate infected systems.
* Evaluate the security of a system or network through penetration testing.
* Provide customized reports outlining options for remediation.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us).

Security Services 

## **Vulnerability Scanning**

Service Description

Scanning an application or system can reveal misconfiguration or vulnerabilities present. Scans are performed against an IT system with an IP address. Reports are generated from these scans that can be provided to developers, administrators or managers describing security vulnerabilities.

What is Included

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.pa.gov](http://www.cybersecurity.pa.gov).

* Vulnerability Scanning
* Vulnerability Reporting

Security Services 

## **Web Application Firewall**

Service Description

Web Application firewalls limits the access to web facing applications located in the Commonwealth’s Enterprise Server Farm’s loadbalaced Web Appliactions Managed Services and Managed Services Light. The reason that application firewalls are needed is to protect the Commonwealth against SQL injections and cross scripting attacks. These attacks are extremely dangerous and can enable attackers to gain access to highly confidential information such as citizen’s names, dates of births, social security numbers, addresses, driver license numbers, etc.

What is Included

* Internet facing critical web applications in the Enterprise Data Center.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.pa.gov](http://www.cybersecurity.pa.gov)

Security Services 

## **Web Application Vulnerability Scanning**

##

Service Description

Scanning a web application can reveal misconfiguration or vulnerabilities present. Scans are performed against a web application. A URL and an IP address are required. Reports are generated from these scans that can be provided to developers, administrators or managers describing security vulnerabilities.

What is Included

* Vulnerability Scanning
* Vulnerability Reporting

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us)

Security Services 

## **Web Content Reporting**

Service Description

Delivers reports, analyze and assess an agency’s internet usage.

What is Included

* Create enterprise level Blue Coat Compliance Reports and provide [RA-Investigations@pa.gov](file:///D%3A/_Blue%20Coat%20Docs/RA-Investigations%40pa.gov) with internet usage reports.
* Help the Agency read and interpret reports that Enterprise Information Security Office provides to the Agency.
* Help the Agency troubleshoot report issues and develop reports to suit the needs of the Agency.

Service Levels

None

Additional Information

Reference documents which provides more in-depth details of this service are available at [www.cybersecurity.state.pa.us](http://www.cybersecurity.state.pa.us)

Software as a Service 

## **Address Verification**

Service Description

Access to web services that clean and verify mailing lists containing street addresses.

What is Included

* Offers a shared service for use by multiple agencies.
* Leverages the OA address verification infrastructure.
* Processes a file containing a single address (one address at a time).
* Processes a batch file that contains multiple addresses.
* Qualifies batch processing of addresses for postal discounts.
* Provides a developer integration guide for integrating applications with the web services.
* Monthly data updates.
* Address Verification Software Updates.
* Maintains 3-5 second web service response time.
* Provides a Graphical User Identification and Password per application.

Service Levels

Availability Service Level Objective:

* Target 99% uptime.

Response Time Service Level Objective:

* **Urgent** –Production service is unavailable – Immediate.
* **High** – Connectivity issue or performance issue – 1 business day.
* **Medium** – Firewall Port to be open – 2 – 5 business days.
* **Low** – Questions or Informational request – 6 to 10 business days.

Additional Information

None

Software as a Service 

## **Alerting and Notifications**

Service Description

Delivers Alerting and Notifications solutions that meet most customer requirements. Alerts can be delivered to several devices, including email, cell phone (text), pager, and home phone.

What is Included

* Assist with the agency development of requirements.
* Assist with the agency on-boarding.

Service Levels

Agreed upon deadline between business owner and development team.

Additional Information

None

Software as a Service 

## **Application Development& Support**

##

Service Description

Delivers business application solutions that meet specific customer requirements.

Note: This service is only available to the consolidated agencies.

What is Included

* Perform the standard tasks of System Development Life Cycle (SDLC).
* Work with business analyst, project and/or end user to gather requirements.
* Work with Project Manager to develop a project plan and determining development methodology (Waterfall, Agile/Scrum or Hybrid).
* Design & build applications that comply with commonwealth standards.
* Design & build applications that address the needs of the customer.
* Perform system coding.
* Integrate application with existing systems.
* Provide data conversion options.
* Ensure adequate application security measures are followed.
* Provide unit testing and quality assurance prior to releasing application for end user acceptance testing.
* Provide documentation and user training options.
* Coordinate production implementation with hosting provider.
* Provide ongoing maintenance and support.

Service Levels

Agreed upon deadline between business owner and development team.

Additional Information

Development Environment:

* .Net (C# VB)
* SharePoint 2013
* CRM (Dynamics) 2013
* Visual Studio (2008, 2010)
* Team Foundation Server (TFS 2012)

Software as a Service 

## **ArcGIS Desktop Tools**

Service Description

Delivers access to centralized pool of ArcGIS Desktop tools and extensions, reducing the need to support and maintain desktop installations of the software across the Commonwealth.

What is Included

* Leverages OA ArcGIS Desktop and Citrix software licenses.
* Provides access to software for the occasional user that needs the tool on a limited basis.
* Makes available storage for users to work with large files directly from the Citrix server.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High- up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

 “Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

Target 99% uptime.

Additional Information

Check ESRI (Environmental Systems Research Institute) web site for training courses – [www.esri.com](http://www.esri.com).

Software as a Service 

## **Daptiv Project Portfolio Management**

Service Description

Daptiv, a cloud-based project portfolio management space, provides the agencies with an automated method for submitting agency project requests, provides a more efficient means of reporting the health of projects to the EPMO, and a tool that is utilized in managing individual projects and an agency’s portfolio of projects.

Requests that meet one or more of the following criteria should be submitted through this process:

* Agency IT projects that are seeking OIT approval as per the parameters defined in [ITP-EPM006 – IT Projects and Project Management](http://www.oa.pa.gov/Policies/Documents/itp_epm006.pdf).
* Agency projects that meet the GOTIME/Government that Works objectives.
* Agency projects which are requesting OA assistance via the Pennsylvania Interactive Office via the Office of Data and Digital Technology, including new websites, web apps or mobile apps.

**Note: This process does not replace the existing mechanism to request services from OIT**

What is Included

* Automated method for submitting agency project requests for approval by OA
* A means to report the health of projects
* Reporting capabilities
* Integration with Microsoft Project
* Integration with Microsoft Outlook

Service Levels

Service level objectives are based on priority, defined by impact and urgency.

Additional Information

Information and documentation regarding the services, including but not limited to training guides and other instructional related information is available on IT Central within the Enterprise Project Management Office persona.

Software as a Service 

## **Geocoding**

Service Description

Access to web services that provide a latitude and longitude for street addresses.

What is Included

Standard features of this service are:

* Offers a shared service for use by multiple agencies.
* Leverages the OA Matchmaker software license.
* Processes a file containing a single address (one address at a time).
* Processes a batch file that contains multiple street addresses.
* Provides the ability to obtain boundary information per point (i.e. what municipality does a point fall within).
* Provides a developer integration guide for integrating applications with the web services.
* Semi-annual data updates.
* Maintains 3-5 second web service response time.
* Provides a Graphical User Identification and Password per application.

Optional features of this service are: Customers may submit a file for geocoding. Under this optional service feature, data field definitions represent the following:

**Address =** Required street address.

**City =** City where Address is located.

**State =** Valid 2-character State abbreviation where the address is located.

**Zip =** 5 or 9-digit U.S. Postal Code of where the address is located.

**RecId=** Record Id (optional).

Service Levels

Priority Levels and Allowable Response Times

* Critical– within 30 minutes to respond to customer
* High– up to 8 hours to respond to customer
* Medium– up to 24 hours to respond to customer
* Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

None

Software as a Service 

## **GIS Data Hosting and Metadata**

Service Description

Delivers access to hardware/software infrastructure to store GIS data for sharing across multi-jurisdictions.

What is Included

Standard features of this service are:

* Leverages the OA Oracle license and database servers.
* Enables data steward/owner to administer data.
* Follows Standard Operating Procedures and Change Management processes for data updates.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

None

Software as a Service 

## **IES ERP Business Application Services**

Service Description

Implements and supports the business applications that are used by the Commonwealth’s central business process owners, primarily running in the SAP environment.

What is Included

The following functions are available in the IES ERP environment:

* **Finance – Controlling** **(FI-CO)** – Recording of Financial transactions including Accounts Payable, Accounts Receivable, General Ledger, Asset Accounting and preparation of Commonwealth financial statements.
* **Financial Management (FM – Budget)** Budget planning, Budget execution.
* **Procurement / Supplier Relationship Management (PROC / SRM)** (includes Live Auction) It is the process of acquiring goods or services. Activities include: Determination of requirements, Requisition, Purchase order, Good receipt/Invoice Received, and Invoice verification and vendor payment.
* **Supplier Relationship Management (SAP SRM)** – Supports the full cycle from source and purchase to pay to spend and supplier performance management. It streamlines operations, enforces compliance with contract and purchasing polices.
* **Plant Maintenance (PM)** Managing and monitoring of Facility and Equipment repair and Maintenance request
	+ Production Planning (PP) - Managing and Monitoring the Manufacturing of Goods
	+ Flexible Real Estate (FRE) - Managing and monitoring of Real Estate Contracts
	+ Sales and Distribution (SD)- Managing of Sales orders, Delivery of Goods and Billing
* **Human Resources (HR**) - Employee Administration, Organization management, HR Administration, Benefits, Time and Attendance.
* **Payroll (PY)** The SAP payroll module calculates the gross through net processing of payroll for employees using data from SAP HR/FI Modules.  This is accomplished through payroll schemas, rules, wage types, and their associated processes.  Payroll produces payroll and financial postings, payment data for Treasury, Third Party vendor payment data, and tax and general reporting.
* **Travel Expenses (TVL)** – Employee Travel Planning and Travel Management.
* **RWD uPerform** (Commonwealth Custom Help, Training Documentation, EUP’s, Simulations, eLearning, etc.)

Service Levels

The contractual SLA with the technical environment provider for system availability to end users is 99%.

Additional Information

Customers should contact Robyne Lyons at roblyons@pa.gov for other information.

Software as a Service 

## **Information Technology Service Management (ITSM) System**

Service Description

The ITSM system service enables organizations to automate their IT support processes. The ITSM system contains a suite of modules designed to automate ITIL process workflows. Services include development and configuration of the ITSM system to meet an agency’s needs. Incident Management and Asset and Configuration Management, Each managed service framework is structured upon best practices found within the Information Technology Infrastructure Library (ITIL).

What is Included

The ITSM system features and support services that agencies can utilize are described below.

Incident Management Service:

* This service automates and transforms information technology for Service Desk incident reporting and resolution.
	+ Allows service desks to receive incident tickets electronically without the need for manual processing. It supports the incident ticket electronically from the time it is reported to the time it is resolved.
	+ Auto-sends customer surveys and service desk reports.
	+ Requirements gathering and documentation support.
	+ Workflow configuration and testing support.

Asset and Configuration Management Service:

* This service automates and transforms asset storage and tracking.
	+ Creates a single system of record for asset/configuration items
	+ Many types of asset/configuration items can be stored.

Maintenance support for IT assets that are covered under the Third-Party Maintenance contract

Service Levels

| **Nature of Defect** | **Production Instance Target Initial Response Time** | **Non-Production Instance Target Initial Response Time** |
| --- | --- | --- |
| Availability Defect | Classified as P1 DefectWithin 30 minutes at all times | Classified as P2 DefectWithin 2 hours at all times |
| Critical Defect | Classified as P2 DefectWithin 2 hours at all times | Classified as P3 DefectWithin 12 hours on ServiceNow business days, excluding holidays  |
| Non-Critical Defect | Classified as P3 DefectWithin 12 hours on ServiceNow business days, excluding holidays | Classified as P4 DefectWithin 24 hours on ServiceNow business days, excluding holidays |
| Other | No target initial response time | No target initial response time |

Additional Information

The Commonwealth’s IT Service Management tool is ServiceNow. This service offering is Software as a Service.

Software as a Service 

## **OneDrive for Business (OD4B)**

Service Description

OD4B is a personal online storage space in the cloud, provided by your organization as part of an Office 365 (O365) subscription. It can be used to store and synchronize work files across multiple devices with ease and security. Users can share their files with business colleagues as needed, and edit Office documents together in real time with Office Online. OD4B provides advantages over typical file shares in supporting versioning, sharing, co-authoring and more. Additionally, the O365 compliance tools can be used with documents in OD4B.

What is Included

* **Store Work Files** – Allows the copy, move, rename and deletion of files from OD4B just like other files in your file system.
* **Sync OD4B** – Allows access to your files from File Explorer on your desktop instead of from a web browser even when you’re not connected to the internet. All updates sync to OD4B or site libraries whenever you’re online.
* **Share Documents/Folders** – Allows sharing from any device by going to your O365 site in a browser.
* **Using Office Online in OD4B** – Allows Office documents stored in OD4B to be viewed and edited in a web browser.

Service Levels

Service level objectives are based on priority, defined by impact and urgency.

Additional Information

Information and documentation regarding the shared service is available at [SP Central](http://spcentral.oa.pa.gov/).

Software as a Service 

## **PA Map Gallery**

Service Description

Delivers access to and/or the creation of commonly used web maps and/or web mapping functionality.

What is Included

* Allows business partners, primarily Commonwealth agencies, local and federal government agencies, law enforcement, and first responders to gain access to commonwealth maps.
* Maps are accessible over the Internet/Intranet.
* Security – Windows authentication against active directory.
* Framework containing commonly used web mapping functionality such as zoom in, zoom out, routing/driving directions, spatial reporting, automatic vehicle tracking, map annotation, secure maps, map user management, and much more.

Service Levels

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

None

Software as a Service 

## **TomTom Tools**

Service Description

Provides access to commercial map data.

What is Included

* Responders, Regional Counter Terrorism Task Forces (RCTTF), regional planning organizations, and K-12 schools and districts.
* Contractors/consultants doing work for these organizations can use the data as long as their client is one of these agencies, and it is used specifically for the specified licensee’s project.
* A letter of understanding (LOU) must be signed by all sub-license parties.

Service Levels

Service Activation:

* Completion of requests within 3 business days.

Priority Levels and Allowable Response Times

1. Critical– within 30 minutes to respond to customer
2. High– up to 8 hours to respond to customer
3. Medium– up to 24 hours to respond to customer
4. Low– up to 48 hours to respond to customer

“Response Time” is defined as the time between receipt of the call and/or ticket and the time that work on the problem begins. Due to the wide diversity of problems that can occur, and the methods needed to resolve them, response time is not defined as the time between the receipt of a call and/or ticket and problem resolution.

Availability Service Level Objective:

* Target 99% uptime.

Additional Information

The components of this offering include:

1) MultiNet with routing attribution, state of PA plus a county buffer of surrounding states

2) StreetMap Premium for ArcGIS Server, nationwide coverage includes United States, Canada, and Puerto Rico

3) MultiNet Administrative Areas, state of PA

4) MultiNet Post (ZIP +4 Centroids), state of PA

5) MultiNet FGDC Metadata

Software as a Service 

## **Web Map Creation**

Service Description

Provides personnel resources for the creation of web maps based on customer requirements.

What is Included

* Work with customer to define requirements such as symbology, colors, labels, etc.
* Requirement and design documents.
* Create web map using commonwealth standard tools.
* Publishing of web maps on the Internet/Intranet.
* Hardware/software infrastructure that is required for web mapping.

Service Levels

Web Map meets the business requirements and design as contained within relevant documents.

Additional Information

Requirements and design phases obtain customer signature to authorize the start of web map development.