Portfolio Office
Quarterly Byte

September 2022

Cybersecurity	**Fiscal Focus**	**Project & Service Updates**
Services & Solutions	**Reminders**	**Did You Know**

Portfolio Office Updates

At Your Service
Please remember that your Portfolio Officer stands ready to assist in your agency's IT needs and priorities. The Portfolio Office is always available for discussions, and you should feel comfortable contacting them about any challenges your organization may be facing so that the Department of Information Technology can engage with possible solutions.

FY2023 Budget & ITMP Review
Thank you to the agency heads and IT leadership that took the time to meet the Portfolio Officers to review your 0876 DoIT services utilization. We hope that you found the meetings to be informative as they were very helpful for the DoIT Team. Your feedback has been distributed to DoIT service teams and the DoIT fiscal office for review. As a reminder, this is the first year that we have engaged in this exercise, and we appreciate your understanding as we continue to work towards our objective of ensuring the FY24 budget accurately reflects the projected utilization of the services that DoIT provides to state agencies.

Project & Service Updates

Statewide Workforce Identity Platform (Okta) Update
Implementation of the Statewide Workforce Identity Platform, Okta, is well underway. Over the upcoming months, DoIT will begin transitioning existing identity and access management tools to Okta starting with SecureAuth. The Connect Maryland Secure Portal (i.e. connect.md.gov) will be transitioned to Okta, resulting in a new user experience. Agency-managed/third-party systems that use SecureAuth for Multi-factor Authentication (MFA) will also be transitioned to Okta. As we move forward, DoIT will share additional details, timelines, and instructions with the impacted agencies/users.   The goal is to complete the transition from SecureAuth to Okta by Dec 31, 2022. Feel free to send questions to DoIT Intake (doit.intake@maryland.gov).

Fiscal Focus

FY2023 Annual Invoice
Information regarding your agency's FY2023 budgeted services has been populated in Apptio. The FY2023 services and quantities represent the estimates at the time the FY2023 budget was prepared. Your agency will be invoiced quarterly (one-fourth of the total annual cost). As a reminder, the IT and Fiscal contacts within each agency are able to access Apptio and this information. For help logging into Apptio or if you have questions about your invoice, contact doitfiscal.billofit@maryland.gov.

IT Solicitation Review
Before issuing solicitations (i.e., RFP, IFB, PORFP, TORFP) for IT products and services outside of an agency's delegated authority, both DoIT and DGS-OSP must review/approve.   Draft solicitations outside of an agency's delegated authority should be sent to DoIT Intake (doit.intake@maryland.gov).   DoIT will review the technical components of the solicitation and, upon approval, route the request to DGS-OSP.   Once the requesting agency has received approval from both DoIT and DGS-OSP, the solicitation can be released to vendors.

Cybersecurity

National Cybersecurity Awareness Month
October is National Cybersecurity Awareness Month and this year's theme is "See Yourself in Cyber." A number of cybersecurity highlights, videos, and information to continually improve our cyber education will be distributed throughout the month.

Statewide Cybersecurity Assessments and Reporting
DoIT's Office of Security Management (OSM) appreciates all the time and effort you and your teams have dedicated to support the Statewide Cybersecurity Assessment initiative this year. A number of agencies have already completed their agency cybersecurity assessment, including both the maturity assessment and external penetration testing. If you have not been contacted regarding either of these phases or the report outcomes, communication is forthcoming. For any additional questions on the status of your report or test, please feel free to reach out directly to the OSM Director of Cybersecurity Initiatives, Karen Poplewski (karen.poplewski@maryland.gov).

Also, new legislation has been passed (SB812 3.5-404-405) to ensure cyber assessments are performed at least every two years and that results are reported up to the OSM. The first report is scheduled to be completed by December 1, 2023. Additional guidance will be forthcoming in late FY23/early FY24.

DoIT Security Operations Center
The DoIT SOC monitors the State's security infrastructure and investigates security incidents 24x7. IT security incidents can be reported to soc@maryland.gov via email, or 410-697-9700.

Highlighted Services & Solutions

MoveIT
MoveIT is a secure file transfer platform for the temporary storage of files to share between entities, whether they are State agencies or external partners. The system meets the State security requirements (password complexity, account expiration, file aging, etc.), and has file retention of 30-60 days, based upon the file retention settings.

eFax
Electronic fax enables the transmission and receipt of a fax via email using your phone, tablet, or computer. Retarus currently provides this service.

Open Data Portal
A self-service platform for hosting and distributing thousands of spatial and non-spatial datasets that can be searched and explored. The Portal meets Maryland's Open Data Act statutory requirements making data easy to find, access, and use.

Private Cloud Hosting Services
A solution for hosting agency applications and data within the state's network with dedicated compute, memory, and storage. The platform is housed in a Tier 3/4 Data Center, which has strict guidelines for maintaining uptime. Additionally, backup copies are stored offsite in a secondary Data Center that can be activated in the event of a disaster.

Security Awareness Training
Security Awareness Training through Infosec Institute InfosecIQ is specifically designed to provide refresher security training in satisfaction with State Finance & Procurement Article 3.5-314. Participants receive monthly security training courses that are engaging, with content that is frequently updated.

Contact your Portfolio Officer if you are interested in learning more about these services.

Reminders

Website Domain Standardization
The use of .com, .org, and .net domains is discouraged and should generally only be used if it redirects to a .gov URL. Contact DoIT prior to purchase and implementation for guidance and approval. State agencies should standardize on the maryland.gov domain whenever possible. Contact your Portfolio Officer if you are planning to implement a new website.

MOU

The DoIT IT Services MOU outlines the roles and responsibilities associated with the recurring services agencies receive from DoIT.   Without an executed MOU, DoIT's ability to provide access to services, contracts, and other resources is significantly hindered. If you have any questions or need a copy of the MOU, contact your Portfolio Officer.

Did You Know

Google Appointment Schedules
The newly released appointment schedules feature lets you share a booking page that makes it easier for anyone to book time with you.

Gmail Users can Report Phishing
Gmail users that receive a suspicious email asking for personal information should report the email for phishing.

1. From your **computer**, go to Gmail
2. Open the email you want to report
3. At the top right, click More
4. Click **Report phishing**

NOTE: *This feature is not available in the Gmail app on IOS and Android*
Phishing emails submitted in this fashion are sent automatically to the DoIT Security Operations Center (SOC) and investigated accordingly.