I. Meeting Call to Order (CIO Jason Clarke)

II. CIO Update (CIO Jason Clarke)

III. Security Update (CSO Solomon Adote)

IV. My.Delaware.gov Project and Communication Update (Dara Schumaier, Organizational Change Management Specialist)

V. Enterprise Projects Supported by Federal Funding Update (COO Jerry Whisman, CPS Justin Day, CTO Greg Lane)

VI. Compliance/Audit Update (CIO Clarke and CSO Solomon Adote)

VII. Public Comment

VIII. Adjournment
CIO Update
Joint Legislative Oversight and Sunset Committee (JLOSC) – TIC Review

- JLOSC Presentation – Tuesday, March 1, 2022
- JLOSC Staff Findings:
  1. The restructuring has limited the period of review, TIC is engaged and involved in topics concerning Delaware government’s information technology infrastructure, effectively performing their statutory duties as an advisory body.
  2. The goals and objectives of the Technology Investment Council are comparable to similar public bodies in other states.
  3. Changes to the current governing statute that would further streamline operations and prevent redundancies:
     - Remove the following language from current statute: “Adopt policies and procedures used to develop, review and annually update a statewide technology plan and provide it to the Governor and the Director of the Office of Management and Budget.”
     - Remove the following language from current statute: “By October 1 of each year, the Council shall provide the Governor and the Director of the Office of Management and Budget with a statewide technology plan. The plan shall discuss the State’s overall technology needs over a multi-year period and the potential budgetary implications of meeting those needs.”
     - JLOSC staff agrees the above duties in TIC’s statute are redundant and effectively performed by DTI and GEAR, the latter of which has significant membership overlap with TIC.
  4. The review observed no issues with FOIA compliance.
  5. Membership includes representation from each branch of Delaware’s government serving by virtue of position.
     - JLOSC staff recommends clarifying quorum requirements in TIC’s governing statute, so any vacancies do not affect quorum.
  6. The limited feedback received from public outreach survey suggests confusion surrounding the purpose of TIC.
     - JLOSC staff recommends adding more information to TIC’s website to help educate the public on the purpose and goals of TIC.
Federal Investments

Technology Modernization $40M
- Mainframe Modernization
- Datacenter Modernization
- Network Modernization
- Security Incident Detection and Response

Digital Government $35M
- Digital Government Platform
- Digital Accessibility (WCAG)
- ServiceNow - Automation & Fulfillment
- Email Phishing Tools
- GIS-Geospatial Datasets
- Citrix - Remote Work
- Public Meeting Sites (Technology Upgrade)

Broadband $110M
- Edge Out (Wireline) Capacity
- Connect DE Students Program Administration

Coronavirus Aid, Relief, and Economic Security (CARES) Act
The American Rescue Plan Act of 2021
Security Update
Did you know...?

- 47% of Americans experienced financial identity theft
- Ransomware is leading the way in cyber security events

Ransomware by the Numbers CLOUDWARDS

**$50 MILLION**

The Largest Ransom Demand

*Made to computer giant Acer in March 2021*

**37%**

OF BUSINESSES

WERE HIT BY RANSOMWARE IN 2021

**IN 2031, RANSOMWARE WILL COST THE WORLD**

$265 BILLION

ON AVERAGE, IT COST BUSINESSES

$1.85 MILLION

TO RECOVER FROM AN ATTACK IN 2021

**32%**

OF VICTIMS

PAID A RANSOM DEMAND IN 2021

ON AVERAGE, PAYING VICTIMS RECOVERED ONLY

65% OF THEIR DATA

**57%**

OF COMPANIES

RECOVERED THEIR DATA USING A CLOUD BACKUP

IN 2021, EVERY

11 SECONDS

A COMPANY IS HIT BY RANSOMWARE
Anatomy of a Cyberattack

- A Web Application was attacked
  - Vulnerability in USAHerds application
- It was detected and thought contained
- A week later CrowdStrike alerted on abnormal connections
- Targeted Domain Administrator accounts
- The attacker found admin jump server with access to 5,000 servers
- They tried to get them out 3 times
- Contacted MS-ISAC and federal partners
- Same attacker identified within multiple state’s computing environment
State of Cyberattack

- **Log4J Vulnerability** – Going after components of most of our software.
  - Used across almost all our Java applications, 500+ & IT tools, even VMware
- **SHIELDS-UP** - Directive from CISA/DHS/FBI
  - State took measures to protect our computing environment from adversarial activities.
  - Block rules implemented to stop traffic from:
    - Cuba, North Korea, Iran, Syria, Sudan, Russia, Ukraine
  - Agencies have the option to request for a specific address of a verified and validated partner to be whitelisted and excluded from this block.
2022 Cyber Predictions

- Direct Attacks & Compromises:
  - Identity and Account Breaches
  - Web Application Breaches
  - Remote Access (VPN) Breaches
- Phishing and Social Engineering attacks will continue
  - 91% of cyber attacks started with phishing email
  - Fake emails that look legitimate, asking for account information.
  - Business Email Compromise (BEC) has been easy money
- Ransomware will lead disruptive cyber attacks
  - Why sell data when they can just get you to pay to get it back?
- Cybercrime proceeds ($105 B), outpaces illegal drugs.
The Identity Service

id.delaware.gov

my.delaware.gov
My.Delaware.gov is Here!

NO IMPACT on Access to May 2022 Open Enrollment!

- Legacy access via URL (https://sso.Delaware.gov/) remains in place through this year’s Open Enrollment.
- Every effort will be toward driving employee access via the more secure my.delaware.gov portal.

Employees...

- use my.delaware to
  - access Employee Self Service (Pay advices, benefits, taxes)
  - view State Pension Annual Statement
  - Access other applications as assigned (e.g. Vaccine/Testing)

- never lose access between state/K12/higher ed jobs (business email changes);
- retain permitted access to tax and pay information after leaving state employment due to separation or retirement.

- STILL USE id.delaware.gov for state work applications such as Outlook, Teams, eStar, etc.
Employee Self Service Migration Team

- DTI Project Staff, CSO, OCM
- OMB/ERP/PHRST
- DHR
- DHR State Benefits Office

OCM Communications Channels

**Web Hosted**
- DTI website (FAQs, Instructional Videos, PDF)
- https://employeесselfservice.omb.delaware.gov/
- **sso.Delaware.gov** ([DE-SSO portal page](https://employeeselfservice.omb.delaware.gov/))
  - Notifications and instructions for diverse user groups
- **ID.Delaware.gov** ([State Employee Okta Tenant](https://employeeselfservice.omb.delaware.gov/))
  - Notification on login; tile appearance changes
- Classlink – changes to LEA access to ESS

**Emails**
- ALL State email blasts ongoing (began mid Nov. 2021)
- Personalized, targeted email direct to employee (Dec. 2021)
- Stakeholder communications (posters, instructions/support)

**Meetings/presentations to stakeholders**
- Delaware Association of School Business Officials
- HR Roundtable
- Charter School Business Managers
- Delaware Association of School Personnel Administrators
- TechMacc (DOE’s monthly meeting for school technology staff)
- PHRST End Users
- Ad hoc with organizations as requested
Timeline – Migration Activities

Ongoing Migration Communications – Assure ALL PHRST-paid employees complete 2 steps:
✓ have a Home Email and an Okta Email Login visible on their Personal Information in Employee Self Service
✓ Register for my.delaware.gov with that same Home email address
  • Notification on id.delaware.gov AND appearance changes to Employee Self Service and DE-SSO tiles directing users to my.Delaware.gov
  • Coordination with DOE to assure similar changes on the K12 side
  • Rosters of employees who have not migrated going to organization HR Reps with instructions on how to help them complete migration
  • Instructions for current/separated users posted on DE-SSO page about changes in access.

On/about 03/01/22 – Single Sign-on access to Employee Self Service, Pensions and other DE-SSO applications are completely assumed by my.delaware.gov.

Note: id.delaware.gov still provides state worker access to work-related applications.

May 2022 Open Enrollment: legacy access still available via URL https://sso.delaware.gov/
KEY CHANGE MESSAGE:

PHRST-paid employees must complete BOTH steps of the 2-step process to access Employee Self Service on my.delaware.gov.
Step 1 – Home + Okta Email Visible on ESS

Log in to ESS (via legacy access URL)

Add a Home Email Address to Personal Information and assure Okta Email Login is visible (may require toggling “Preferred” flag and re-saving the record)

Step 2 – Register on https://my.delaware.gov

Coming after 2/22/22: Improved my.delaware.gov landing page:

- Register Now button
- Forgot Password help
- Registration help

Employee Self Service and other assigned tiles appear AFTER PHRST and my.Delaware.gov systems have fully synced—usually 48 hours after registration, UNLESS:

- my.delaware.gov Legal Name doesn’t match PHRST (e.g., hyphenated last name; suffix in the last name field in PHRST but not in my.delaware.gov)
- Okta Email Login missing in PHRST (e.g., incomplete step 1 user did not add a Home Email type or did not toggle “preferred” flag to invoke appearance of Okta Email Login field)
CARES Act Funding

Cabling & Switch Replacement

$16,806,000

- 134 Buildings
- 25 Agencies
- $2.1+M in Savings
- Upgraded State bandwidth from 30GB to 40GB with infrastructure capabilities to support 100GB
Grantham Lane and Carvel Building Before & After
Remote Work: Continuing Impact

Remote-In VPN = 15,000 accounts
Always On VPN = 4,080 accounts
**Key Accomplishments**

- Voted to recommend establishing a position of Geographic Information Officer (GIO) for coordination and governance of GIS technology, including imagery
- Acquired ARPA funding to establish a current (Year 1) baseline for all datasets

**Next Steps**

- Complete flyovers and refresh datasets
- Decision on recommending an annual fund to keep datasets current (~$420K/Yr.)
- Acquire/fill GIO Position

---

**GIO Value / Key Deliverables**

- Develop a statewide GIS Technology strategic plan, positioning agencies and entities to use data collaboratively and strategically
- Align standards and requirements amongst agencies to enable flyover contracts to be consolidated, and reduce/eliminate agency specific flyovers
- Develop/manage GIS budget, including imagery, and foster an ongoing relationship with IT System and Flyover vendors
- Ensure collaboration with the Office of State Planning Coordination (OSPC) to align technology/imagery governance with OSPC-led governance of agency, county, municipality use of GIS systems and imagery

---

**Sample Data Collection Timeline for a 6-year contract (~$2,510,000 or $420k per year)**

<table>
<thead>
<tr>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Year 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$920,000</td>
<td>$130,000</td>
<td>$280,000</td>
<td>$770,000</td>
<td>$280,000</td>
<td>$130,000</td>
</tr>
</tbody>
</table>

- Aerials
- LiDAR
- LULC

---

**Estimated Costs**

- Imagery: $130,000
- LiDAR: $640,000
- LULC: $150,000
- Total: $920,000

**Last Refresh: 2017**
DTI Compliance and Audit Summary (February 2022)
<table>
<thead>
<tr>
<th>IRS</th>
<th>HIPAA</th>
<th>SOC</th>
</tr>
</thead>
</table>
| • Review every 3 years  
• 70+ hours of prep  
• Post audit will account for approximately 20% of resources to identify and develop corrective action plan  
• High to moderate findings, some still pending from 2018 audit | • Review every 3 years  
• 30+ hours of prep  
• Post audit will require the outcome of the Secure End User Services centralization of OMB/DHR to address security findings  
• Moderate to low findings | • Review yearly  
• 25+ hours of prep  
• Post audit will account for approximately 10% of resources to identify and develop corrective action plan  
• Moderate to low findings |
## Recurring Themes/Findings All Audits

<table>
<thead>
<tr>
<th>Governance &amp; Oversight</th>
<th>Technical Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of policy and standards</td>
<td>Requires resources and cost analysis for some findings</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>• Patch Management – Policy should mandate updates, timing and chargebacks to Agencies</td>
<td>• Patching and System Updates – Technology debt</td>
</tr>
<tr>
<td>• Vulnerability Scanning - under development</td>
<td>• Workstation logging – modernize audit logs for trending, retention and review</td>
</tr>
<tr>
<td>• Boundary Protection – risk assessment</td>
<td>• Administrator rights – privileged role overhaul. <strong>Limit rights to job requirements and modernize</strong></td>
</tr>
<tr>
<td>• Risk Assessments Program – formalize requirements, determine staffing needs</td>
<td>• Vulnerability Scanning – explore automated process in lieu of manual launch</td>
</tr>
<tr>
<td>• Access Controls – lifecycle management, hire to separation, modernize requirements, possibly through Service Now</td>
<td>• Configuration Standards: Windows administrators workstations not configured properly – risk assessment review to identify workstations requiring updates,</td>
</tr>
<tr>
<td>• Retention and Recovery – 7-year retention on logs and compliance related data (storage capacity)</td>
<td>• Internal Email Systems- Currently being deprecated</td>
</tr>
<tr>
<td>• Contracts lacking compliance requirements such as exhibit 7 language and onsite audits</td>
<td>• DTI and Agency Partner network protection capabilities not configured in accordance with Pub 1075</td>
</tr>
<tr>
<td></td>
<td>• Compliance and Audit Tools – Edgile audit tool development underway</td>
</tr>
</tbody>
</table>
Public Comment
Contact Information:

Jason Clarke, Chief Information Officer
Jason.Clarke@delaware.gov

(302) 739-9500
DTI.Delaware.gov