# Technology Investment Council

February 23, 2022

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

Coronavirus Aid, Relief, and Economic Security (CARES) Act

INFRASTRUCTURE INVESTMENT & JOBS ACT

The American Rescue Plan Act of 2021

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

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

| 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) |

# Security Update

# Security Update

**Did you know…?**

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

Hellenic Shipping News Worldwide

Bracing for Cyber War: The Global Ramifications of Rising Tension Between Russia and Ukraine

Recent cyber attacks on Ukraine from Russia have suggested the possibility ... Several cyber espionage actors have been working to inflict...

1 week ago

Computerworld

Will World War III begin in cyberspace?

People die because of cyber wars, even if no bullets are ever fired. Instead, they die in emergency rooms that no longer have power,...

3 weeks ago

Deseret News

Cyberwar: What cyberattacks say about the future of war

"Cyberespionage is going on all the time," said Steinberg. Like cyberattacks, cyberespionage could have military or civilian targets. It could...

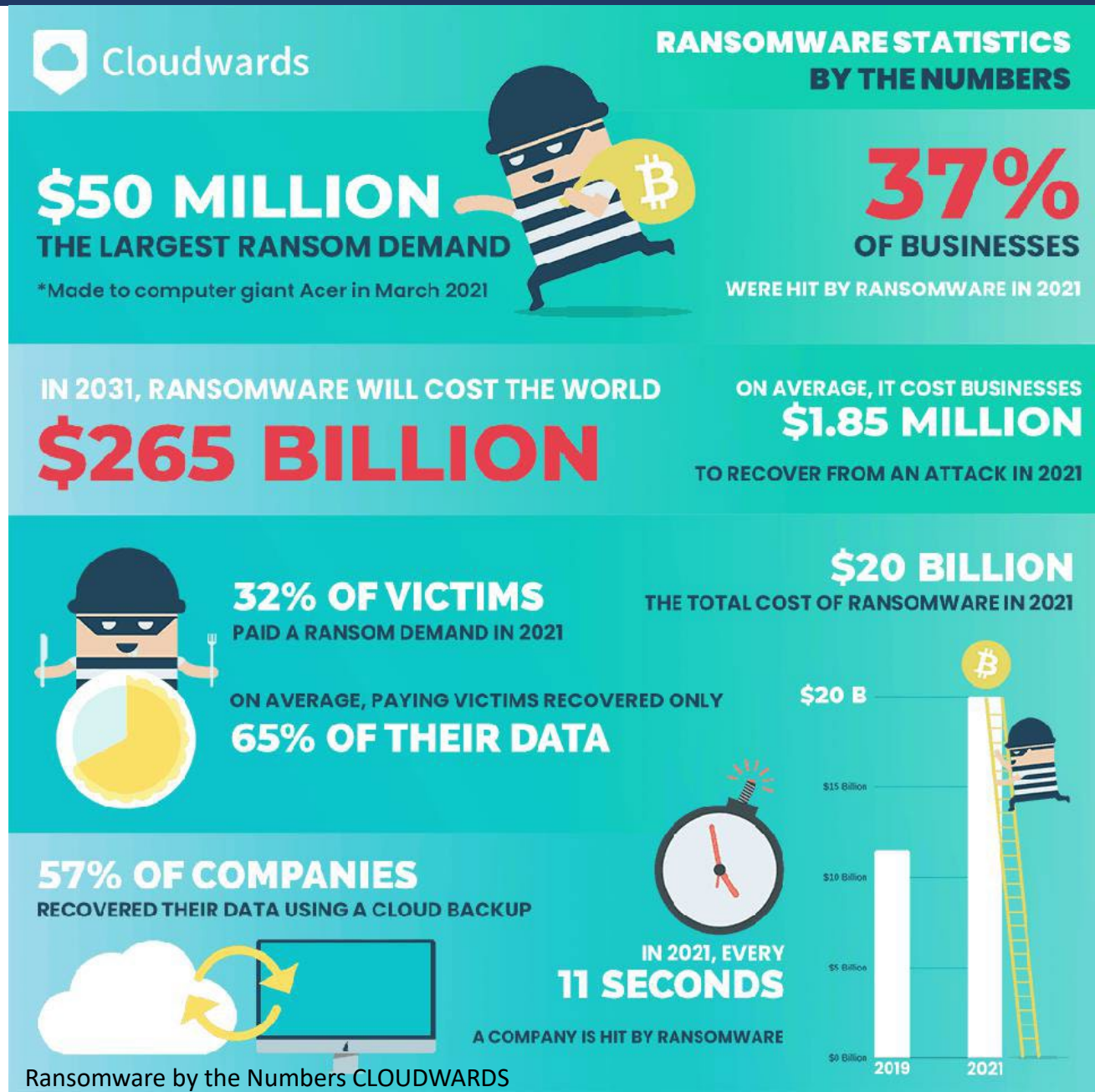
Aug 11, 2021

Forbes

Is The World Ready For A Cyberwar ?

Only a few cyberattacks get classified as cyberwar, while the rest are classified as cybercrime. ... Cyber Espionage Vs. Cyberwar.

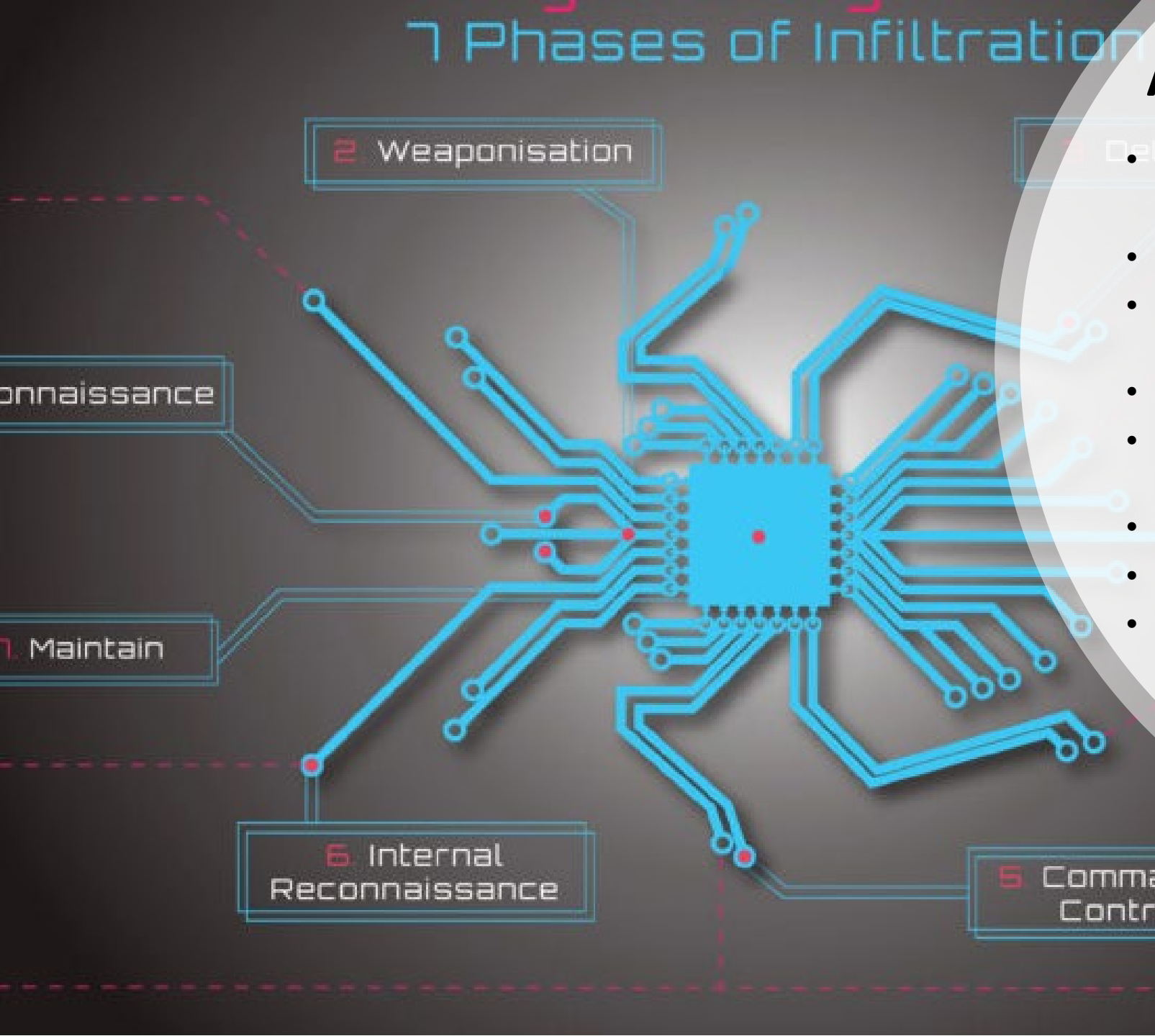
Aug 30, 2021




Ransomware by the Numbers CLOUDWARDS

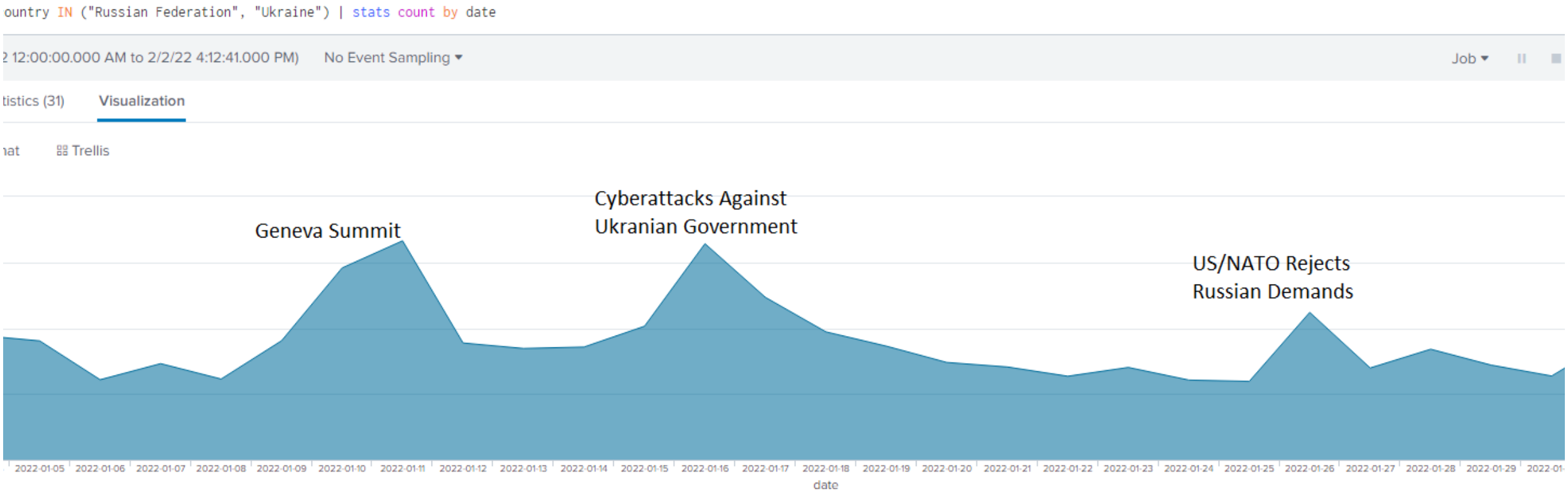
# Anatomy of a Cyberattack

- 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

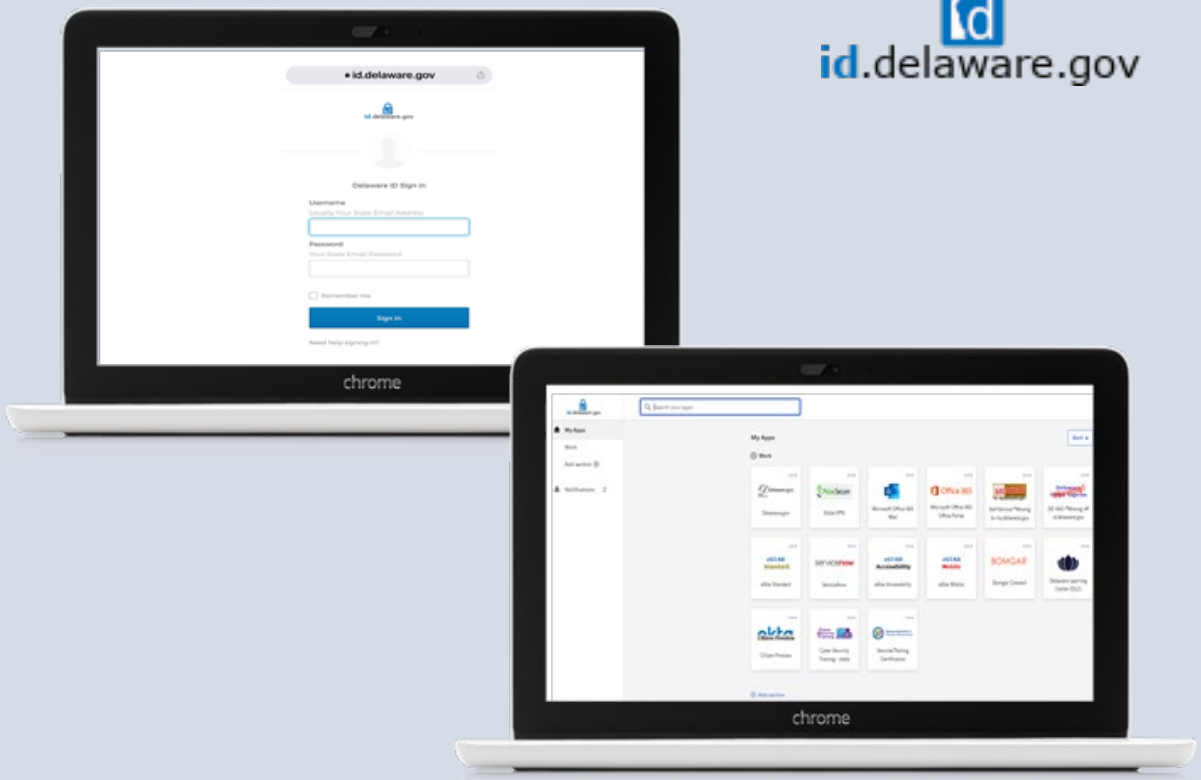
- **Log4J Vulnerability** – Going after components of most of our software.
  - Used across almost all our Java applications, 500+ & IT tools, even VMware
- **SHIELDS-UP -** Directive from CISA/DHS/FBI
  - State took measures to protect our computing environment from adversarial activities.
  - Block 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.

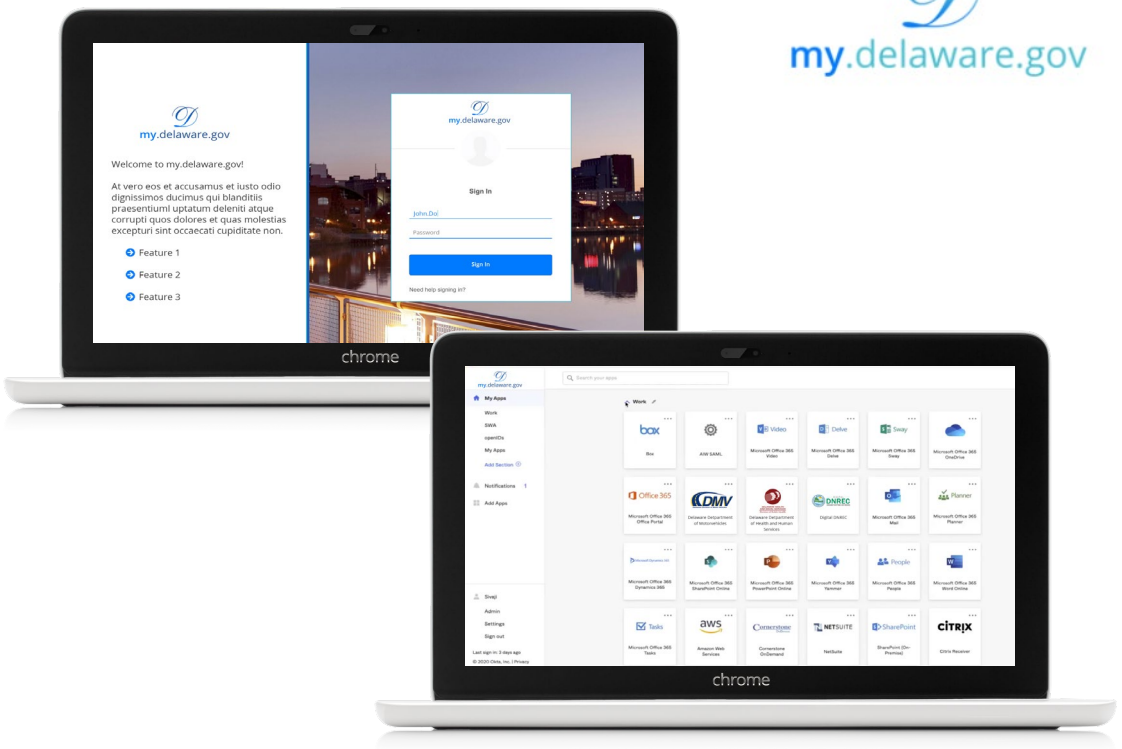


# 2022 Cyber Predictions

- **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 (<u>$105 B</u>), outpaces illegal drugs.**

# The Identity Service



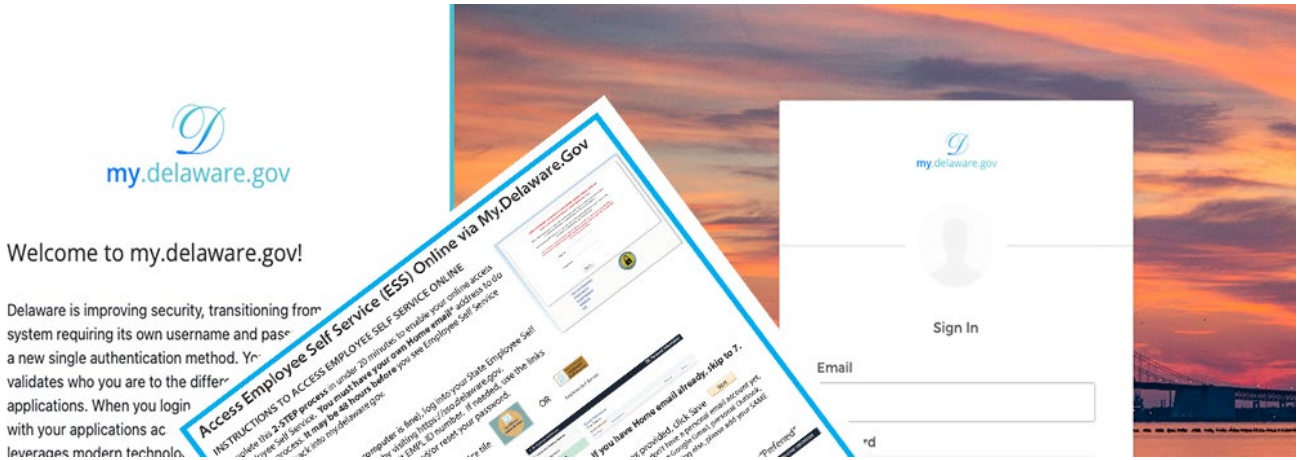
# My.Delaware.gov is Here!

## 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 ec 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.



# OCM – Communications Partnerships & Channels

**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://employeeselfservice.omb.delaware.gov/

- ***sso.Delaware.gov*** *(DE-SSO portal page)*
  - Notifications and instructions for diverse user groups
- ***ID.Delaware.gov*** *(State Employee Okta Tenant)*
  - 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:**

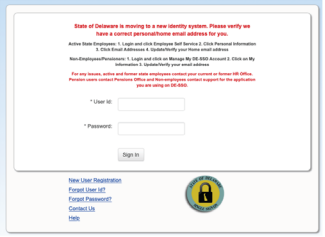
PHRST-paid employees must complete **BOTH steps** of the **2-step process** to access Employee Self Service on my.delaware.gov.

# Step 1 – Home + Okta Email Visible on ESS

## Access Employee Self Service (ESS) Online via My.Delaware.Gov

### INSTRUCTIONS TO ACCESS EMPLOYEE SELF SERVICE ONLINE

Complete this **2-STEP process** in under 20 minutes to enable your online access to Employee Self Service. **You must have your own Home email*** address to do this 2-step process. **It may be 48 hours before** you see Employee Self Service when you log back into my.delaware.gov.



### STEP 1

1. **Using a computer (work computer is fine)**, log into your State Employee Self Service via your Delaware ID or by visiting https://sso.delaware.gov.
Your DE-SSO User ID is your six-digit EMPL ID number. If needed, use the links below the sign-in to get your User ID and/or reset your password.

2. Click on State of Delaware Employee Self Service tile OR
Employee Self Service

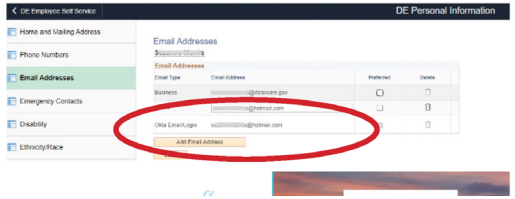
3. Click on Personal Information

4.. Choose Email Addresses (3rd item on the lefthand list).

5. IF you **do not have Home email**, Click the Add Email Address button. **If you have Home email already, skip to 7.**

6. Select **Home** as the Email Type and enter your personal/home email in the box provided, click Save
*__NOTE:__ This email address must be yours alone--not shared with another SOD employee. If you don't have a personal email account yet, you can create a free email account to use for this process (using a state-owned computer is fine). It can be Google Gmail, personal Outlook, Apple iCloud or any free email service. **Also, if you ALREADY registered for my.delaware** to access something else, please add your SAME email you registered for in my.delaware email as your Home email to assure getting your ESS access.

7. VERIFY that you now see "Okta EmailLogin", and it MATCHES your Home Email.
**If you did not have to add Home email, AND DO NOT SEE an "Okta EmailLogin" field, uncheck** your "Preferred" email by checking any other email as "Preferred"--temporarily, SAVE.
Then change "Preferred" back to the address you want the State to use, SAVE again.
**OktaEmail should never be checked "preferred."**



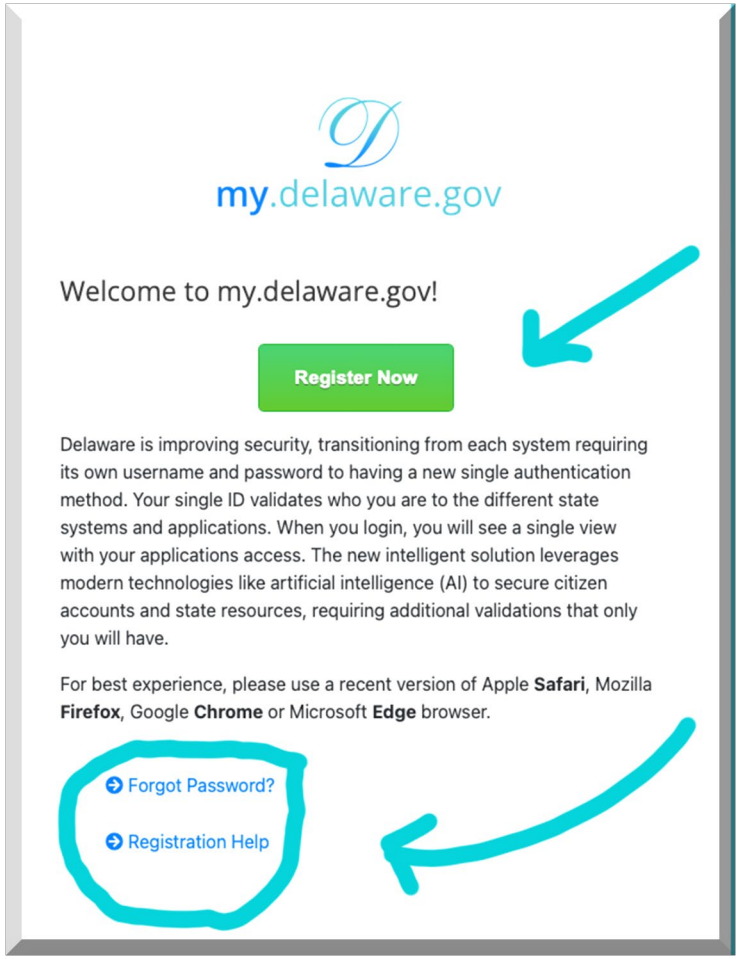
8. **Log Out** of Employee Self Service.

**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)

Detailed instructions and videos: **https://bit.ly/3L7DmS1** or **https://dti.delaware.gov/digital-innovation/my-delaware-gov/my-delaware-gov-faq/**

# 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)

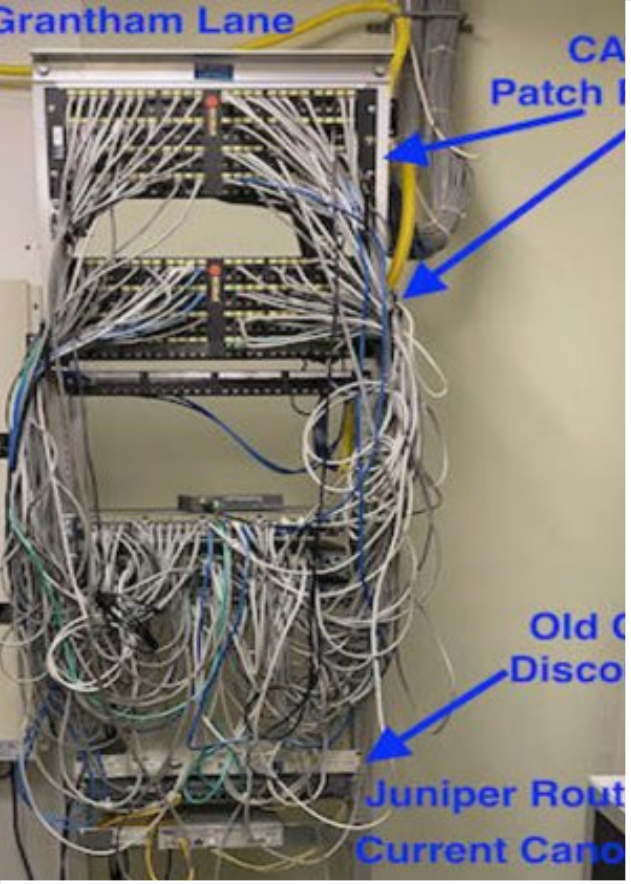
# Enterprise Projects

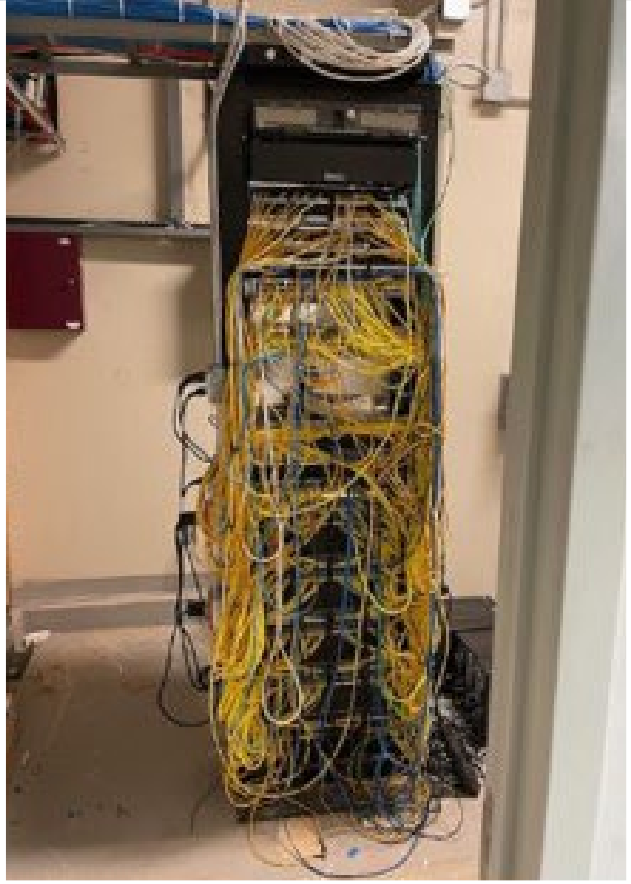
# CARES Act Funding

## 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



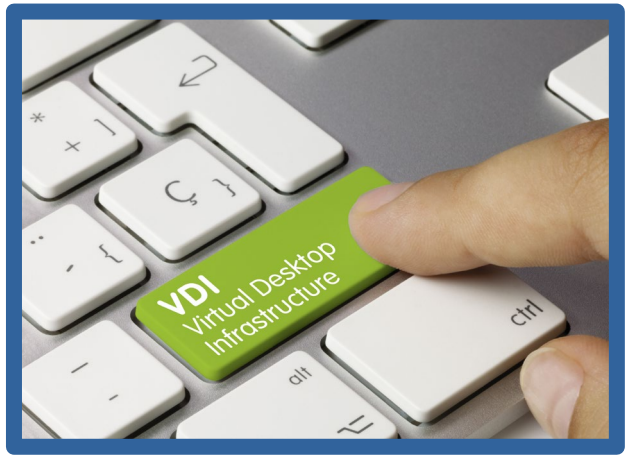


# Grantham Lane and Carvel Building Before & After

# Remote Work: Continuing Impact

**Remote-In VPN = 15,000 accounts**

**Always On VPN = 4,080 accounts**



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

ARPA Funding 2022

| Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 |
|---|---|---|---|---|---|
| $920,000 | $130,000 | $280,000 | $770,000 | $280,000 | $130,000 |
| • Aerials<br>• LiDAR<br>• LULC | • Aerials | • Aerials<br>• LULC | • Aerials<br>• LiDAR | • Aerials<br>• LULC | • Aerials |

Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec

|← FLIGHT →| WINDOW

|← Secure Funding →| Release RFP

|← Vendor Contract →| Deadline

**Estimated Costs**

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

Last Refresh: 2017

## 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

# COMPLIANCE

NASCIO
Representing Chief Information Officers of the States

**Harmonize Disparate Federal Cybersecurity Regulations**

# DTI Compliance and Audit Summary (February 2022)

# 2022 Planned Regulatory Audits

| IRS | HIPAA | SOC |
|---|---|---|
| • Review every 3 years<br>• 70+ hours of prep<br>• Post audit will account for approximately 20% of resources to identify and develop corrective action plan<br>• High to moderate findings, some still pending from 2018 audit | • Review every 3 years<br>• 30+ hours of prep<br>• Post audit will require the outcome of the Secure End User Services centralization of OMB/DHR to address security findings<br>• Moderate to low findings | • Review yearly<br>• 25+ hours of prep<br>• Post audit will account for approximately 10% of resources to identify and develop corrective action plan<br>• Moderate to low findings |

# Recurring Themes/Findings All Audits

## Governance & Oversight

Lack of policy and standards

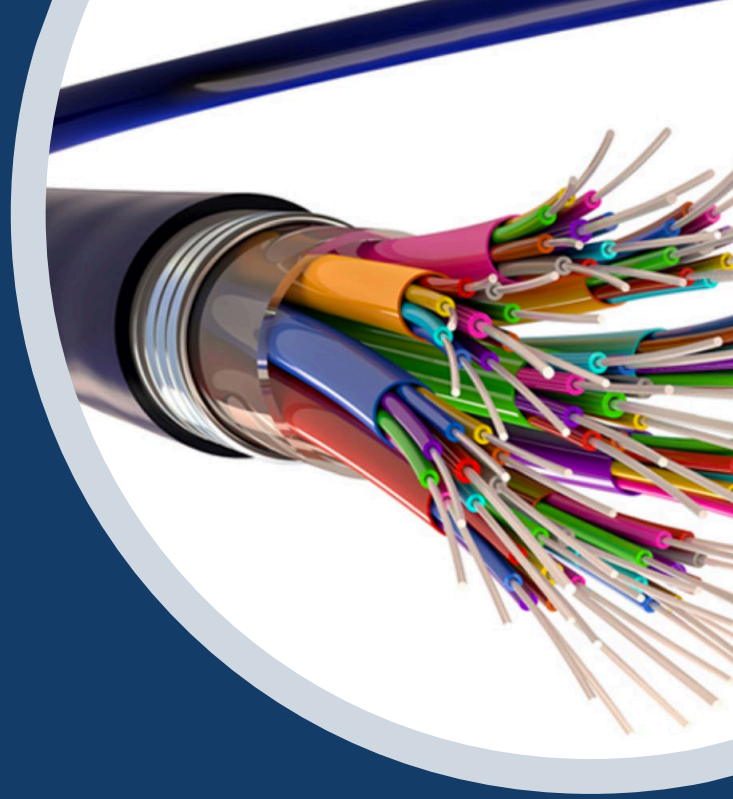
- Patch Management – Policy should mandate updates, timing and chargebacks to Agencies
- Vulnerability Scanning - under development
- Boundary Protection – risk assessment
- Risk Assessments Program – formalize requirements, determine staffing needs
- Access Controls – lifecycle management, hire to separation, modernize requirements, possibly through Service Now
- Retention and Recovery – 7-year retention on logs and compliance related data (storage capacity)
- Contracts lacking compliance requirements such as exhibit 7 language and onsite audits

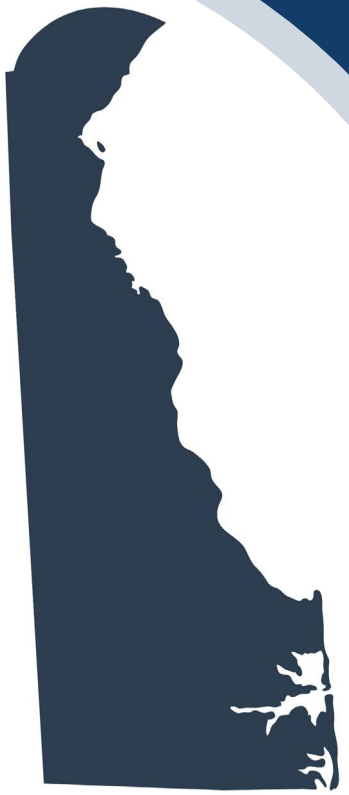
## Technical Requirements

Requires resources and cost analysis for some findings

- Patching and System Updates – Technology debt
- Workstation logging – modernize audit logs for trending, retention and review
- Administrator rights **– privileged role overhaul. Limit rights to job requirements and modernize**
- Vulnerability Scanning – explore automated process in lieu of manual launch
- Configuration Standards: Windows administrators workstations not configured properly – risk assessment review to identify workstations requiring updates,
- Internal Email Systems- Currently being deprecated
- DTI and Agency Partner network protection capabilities not configured in accordance with Pub 1075
- Compliance and Audit Tools – Edgile audit tool development underway

# Public Comment





# Contact Information:


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

**(302) 739-9500**
DTI.Delaware.gov