Technology Investment Council (TIC) — Purpose and Members

- CIO Jason Clarke, Department of Technology and Information*
- Chief Justice Collins Seitz, Supreme Court
- Secretary Jeff Bullock, Department of State
- Secretary Nathaniel McQueen, Jr., Department of Homeland Security*
- Secretary Nicole Majeski, Department of Transportation*
- Secretary Molly Magarik, Department of Health and Social Services*
- Secretary Rick Geisenberger, Department of Finance
- Director Cerron Cade, Office of Management and Budget*
- Controller General Ruth Ann Jones, Delaware General Assembly*

* New Members
Role of The Council

- **Adopt policies and procedures** used to develop, review and annually update a **statewide technology plan**

- **Provide statewide technology plan by October 1** of each year to the Governor and the Director of the Office of Management and Budget

- **Make recommendations regarding the funding of technology** for the coming fiscal year

- **Forward funding recommendations** to the Governor

- **Enforce active project management, review the progress of current projects** to determine if they are on budget and have met their project milestones, and when necessary, recommend the termination of projects

- **Identify opportunities to leverage expertise** in strategically important areas of information technology by partnering with the private sector
Produce reports, dashboards, cyber security/risk profile, MPQR updates related to TIC-recommended projects.

Leverage the power of this committee to make enterprise recommendations to the Governor and GEAR (e.g., life cycling, major projects, innovation, efficiencies).
Our ability to respond and pivot quickly corresponds directly to our capacity to leverage centralized services across the enterprise.

Centralization provides equity, capacity planning, security and interoperability.
Digital Government – Next Generation

Citizen Focused | Secure | Flexible | Integrated

Develop a strategy and roadmap for digital transformation of citizens’ interactions with state government – anytime, anywhere, from any device

- Personalized User Experience
- One Logon/Profile (Fraud Mitigation)
- Services from Any Agency
- One Payment Process
- Modern Payment Options
- Multiple Engagement Options

Let Technology Navigate Government!
Digital Government – Status

• Several agencies have active Digital Transformation projects in progress

• Covid-19 has accelerated digital use and expectations

• Key Foundational Item in progress: OKTA Identity & Access Management/One Logon

• OST, DOS, DTI and others issued joint RFP October 2020
  - Citizen Experience – web & application, legacy system integration
  - Payment Gateway Systems – point of sales machines & software
  - Merchant Processing – bank to bank/credit/debit/ACH processing
  - Reconciliation and Account Analysis – automated bank statement analysis

• 5 of 12 RFP Respondents – additional evaluation sessions May-June 2021

• Project Cost/Funding TBD – transaction funding models vary and require flexibility

• Expect multi-year, phased implementation
Cyber Security Update
Did you know...

- **The number of cyber attacks is going UP not down**
  - 71% of breaches were financially motivated; 25% espionage

- **Ransomware** is leading the way in cyber events
  - Why sell your data when they can just get you to pay to get it back?
  - Baltimore currently impacted by Robbinhood; $18 million spent so far

- **91% of cyber attacks started with a phishing email**
  - Fake emails that look legitimate, asking for passwords/credit card details. 62% of business experienced this in 2018

- **Cyber-crime damages could reach $6 trillion**
  - Up from $3 trillion just two years ago

- **93% of breaches could have been avoided with Basic Cyber-Hygiene**

---

**Cyber Hygiene Essentials**

You can’t afford to not do these

- **1 Protect Your Identity**
  - Protect all your accounts including email, banking, social media and others. Set strong passwords. Turn on multi-factor authentication.

- **2 Stop Virus Attacks**
  - Maintain up-to-date anti-virus software.

- **3 Keep Data Safe**
  - Backup regularly. Ensure your data is always protected (encrypted). Keep a copy of your data somewhere else.

- **4 Be Cyber Aware**
  - Learn how to stop the bad guys. Know their tricks and sneaky ways like phishing and social engineering. Stay safe online and think before you click.

- **5 Stay UpToDate**
  - Keep your devices up to date. Ensure devices like wi-fi routers, smart phones and tablets are running the latest version and are configured securely.

https://de.gov/dcsac
National State of Cybersecurity

• **Supply Chain Compromise; SolarWinds Attack**
  • Break into trust software and have victims download the malware themselves
  • They got in federal agencies, local government and even Microsoft

• **School Attacks**: Ransomware Attacks on Baltimore county, Connecticut, more ([map of attacks](https://example.com/map))

• **State networks and web sites under attack**
  • Defacement, ransom, blackmail and site [weaponization](https://example.com/weaponization)

• **56 % increase in local government targeting**: Baltimore, Atlanta, New Orleans

• **Law Enforcement targeting**
  • DOJ Illinois, Capitol Metro PD attack, DIAC database compromise

• **Elections targeting**
1. Phishing
2. Ransomware / Malware
3. Hacking
4. Web Application Attacks
5. 3rd Party Service Risk
6. Data Leakage
Potential Impact

**Significant Citizen services impact**
- Education System shutdown for weeks
- Law enforcement services disruption
- Health services interruption
- Transportation safety services compromise

**Potential inability to recover some systems rapidly**
- Disaster Recovery on only limited enterprise systems
- Some systems don’t even have current fully skilled support resources

**Weaponization of state services**
- State data used to target systems physically and for fraud
- State web sites used to infect unsuspecting citizens
### How TIC Can Help...

| Address Technology Debt; aged and unsupported critical systems and applications |
| Drive **Cyber-Hygiene** across state government through **Centralization** |
| - Achieve consistent patch levels, security tools and risk levels on systems |
| Ensure new initiatives align to new **Security strategy and program** |
| Drive **Cyber-Hygiene** across state government through **Centralization** |
| - Achieve consistent patch levels, security tools and risk levels on systems |
| Help drive visibility into threats, vulnerabilities and overall risks across state services |
| An **identity-driven**, risk-based security controls framework to protect and deliver a translucent AND effective working environment that can enable our state agency partners To provide services that enhance the lives of Delaware’s citizens. |
| Cybersecurity program resourcing and funding |
IT Centralization Update

**Impacted By COVID**
- Assessments
- Staff Reallocation
- Chargeback
- Service Level Agreements
- Service Catalog
- Procurement

**Interim Focus Areas**
- Controls
- Position Profile Modernization
- ServiceNow Service Catalog
- OMB (budget process to address funding gap)
- Secure End User Package
Secure End User Package

- Network & Connectivity
- Infrastructure (Storage/Backup)
- Enterprise Voice
- Service Desk/Support
- Collaboration Services (Email & Productivity Suite)
- Device (Desktop/Laptop)
Public Comment/Questions