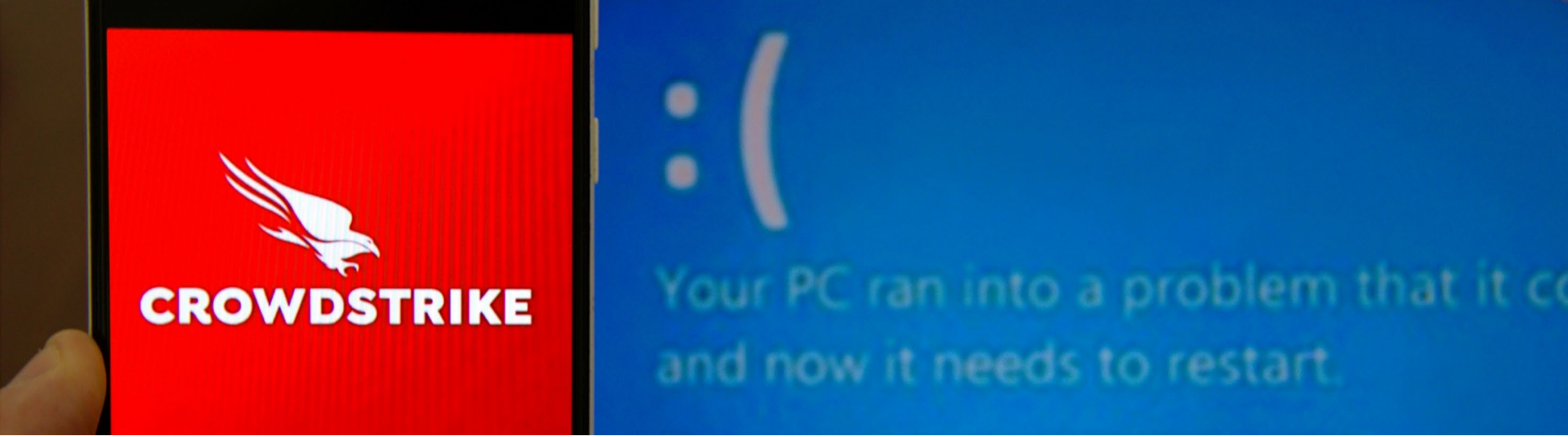
Minnesota IT Services – Cybersecurity Updates for Legislative Commission on Cybersecurity

John Israel | Assistant Commissioner and Chief Information Security Officer (CISO)

MINNESOTA IT SERVICES



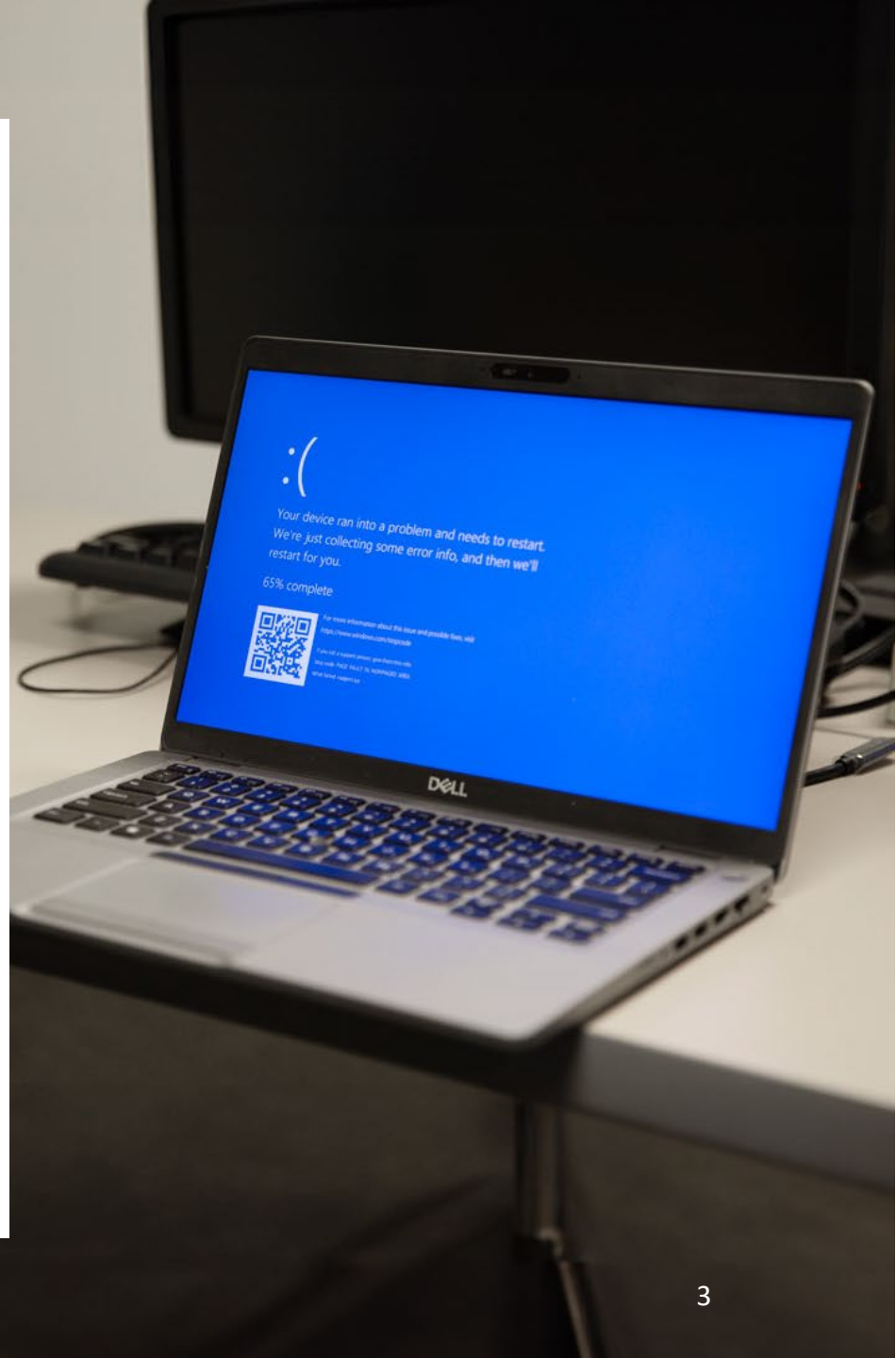
CrowdStrike State of Minnesota Impact

John Israel | Chief Information Security Officer

MINNESOTA IT SERVICES

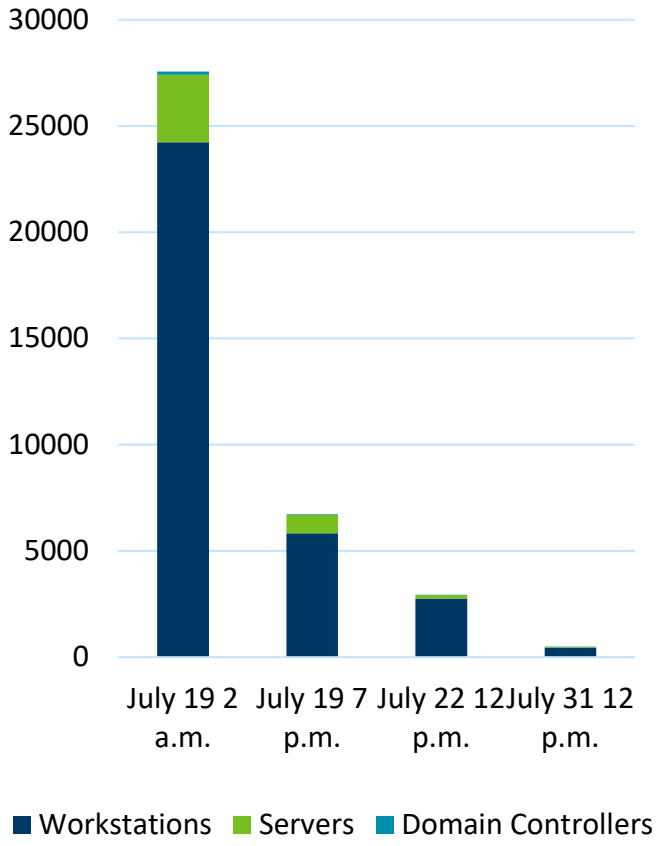
Outage Overview

- **What**: Security vendor CrowdStrike released an update that impacted Windows devices
- **When**: Started midnight Friday, July 19. Most public impact recovered in first 18 hours.
- **Who**: Impacted call centers, applications and websites, VPN, and networks
- **How**: Over 27,000 State of Minnesota laptops, desktops, and servers received the “blue screen of death”

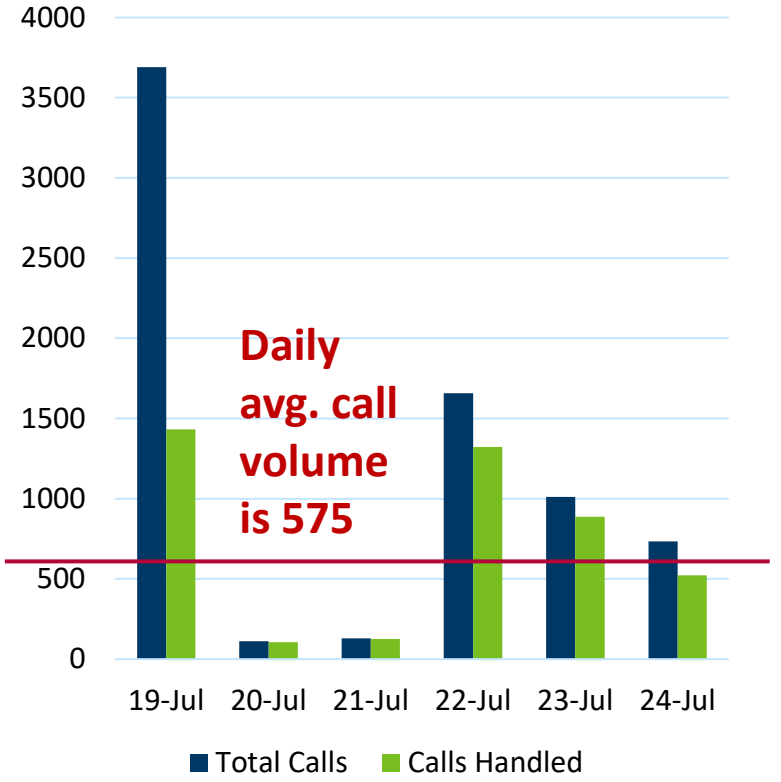


CrowdStrike blue screen response by the numbers

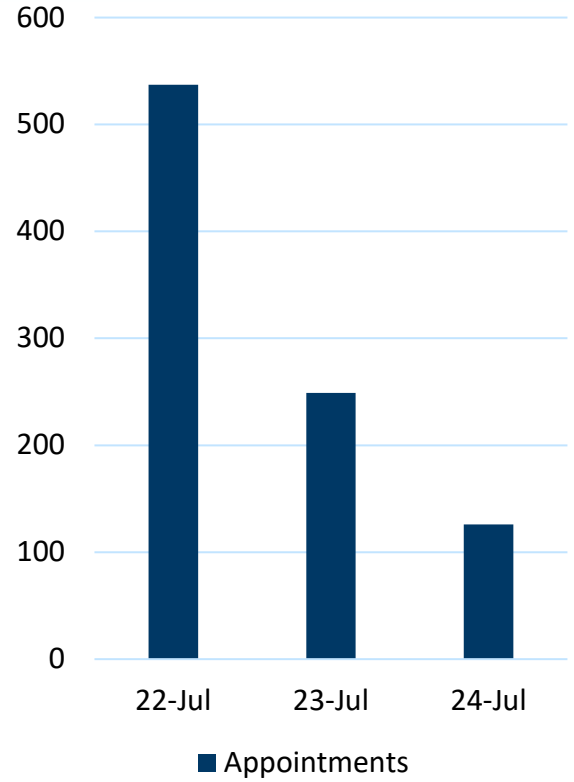
Devices Impacted by Outage



Calls to the MNIT Enterprise Service Desk



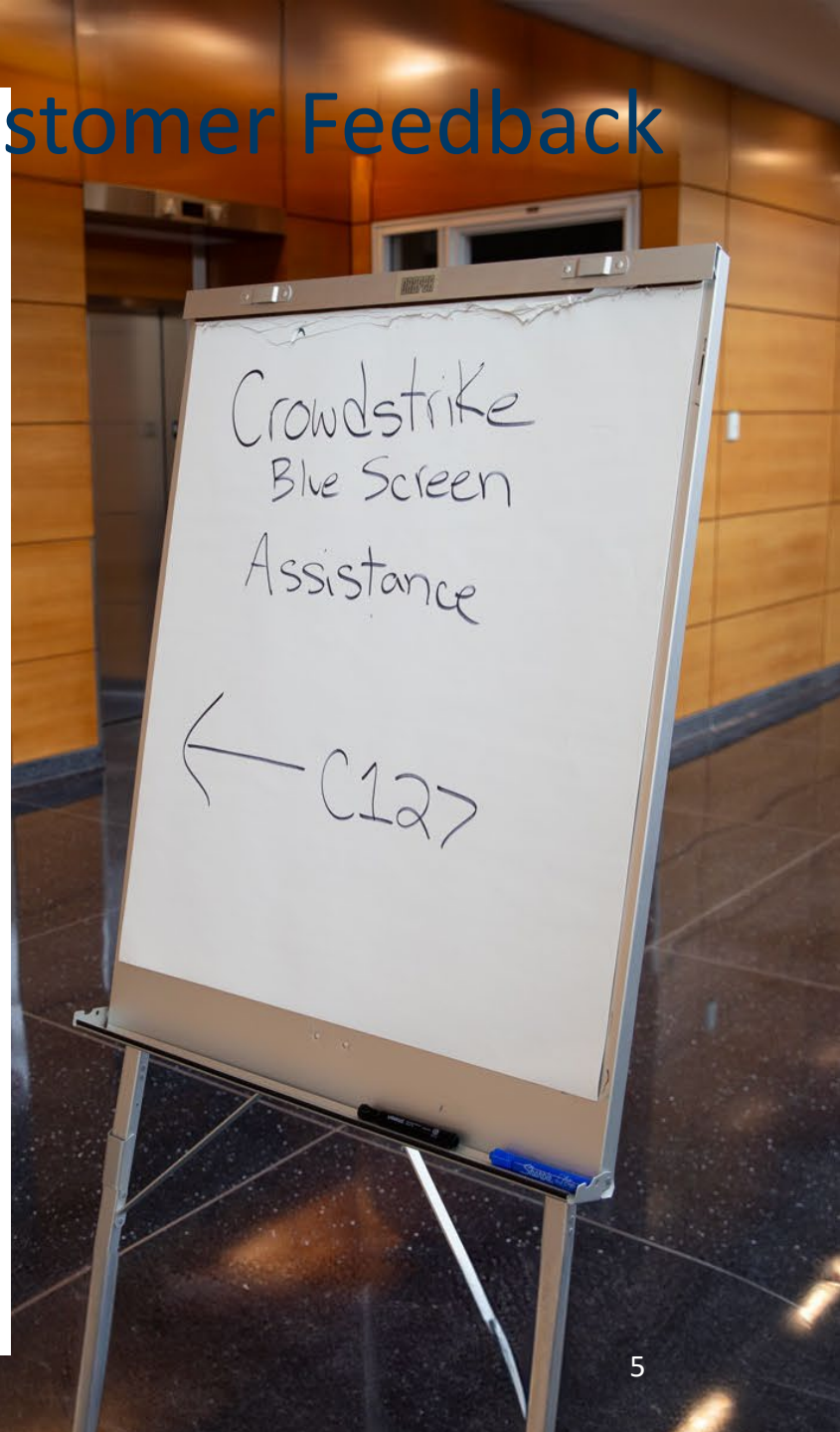
Workstation Appointments



Customer Feedback

> They were following an **easy process** – sign in, sit anywhere, and leave the rest in their capable hands! All I needed to do was login afterwards to make sure I was flawlessly back online.

> My total time at Lafayette was about **15 minutes**. During that time, there was a steady stream of employees coming in and I could see by their faces that they also took comfort in the overall **helpful, efficient vibe** coming from the room and those who were experiencing it.



Next Steps

- Table-top exercises have incorporated issues and lessons learned from this incident
- Continue to incorporate lessons learned into upcoming COOP/DR workshops and tabletop exercises this fall
- Implementing lessons learned from after action into operational changes that will mitigate potential future impact

Cybersecurity Incident Reporting Update

John Israel | Chief Information Security Officer

MINNESOTA IT SERVICES

Cybersecurity Incident Reporting Update

MNIT and BCA are collaborating with partners as we approach deadlines outlined in section 16E.36 of the Public Safety and Judiciary Omnibus law.

- Shared draft form and guidelines with 500+ likely reporting public entities for comment and feedback.
- Feedback from 60+ entities helped with creating a user-friendly process and ensuring we collect the necessary information.
- Reporting form and instructions nearly complete.
- Continue to explore more robust incident reporting opportunities that reporting entities are looking for.

Cybersecurity Incident Reporting Update, cont…

Sept. 30, 2024: Initial version of reporting tool and guidance will be available on MNIT's website.

Dec. 1, 2024: Public agencies are required to report cybersecurity incidents.

- **Who reports:** Public agencies: Any public state agency, political subdivisions; school districts, charter schools, intermediate districts, cooperative units, and public postsecondary education institutions. Government contractors or vendors that provides goods or services to a public agency must report an incident to the public agency.
- **When reports must be made:**
  - Within 72 hours of when incident was identified or occurred.
  - Within 24 hours if Criminal Justice Information is impacted.

Cybersecurity Incident Reporting Update, cont…

Sharing information benefits:

Minnesotans

- Helps provide a better understanding of the nature of and impacts from cybersecurity events to keep services available to Minnesotans and protect their data.

MNIT and BCA

- Gain awareness of the scope of the incidents.
- Assist other organizations in defending their IT resources.
- Understand how bad actors bypass security controls.

Public Entities

- MNIT and BCA may share cybersecurity threat advisories or general guidance to help other local governments defend against cybersecurity threats.

Legislators and Public Leaders

- Improve quality of data related to cybersecurity risk.
- Highlight potential gaps that require resources to mitigate risk.

Constituent Identity and Access Management

John Israel | Chief Information Security Officer

MINNESOTA IT SERVICES

Login.mn.gov

- Constituent **identity** and access management portal.
- Improve security, reliability, and availability of services to Minnesotans.
- Enhance fraud detection capabilities.
- Enrich constituent and partners experience at a lower cost structure.

Benefits to State Agencies

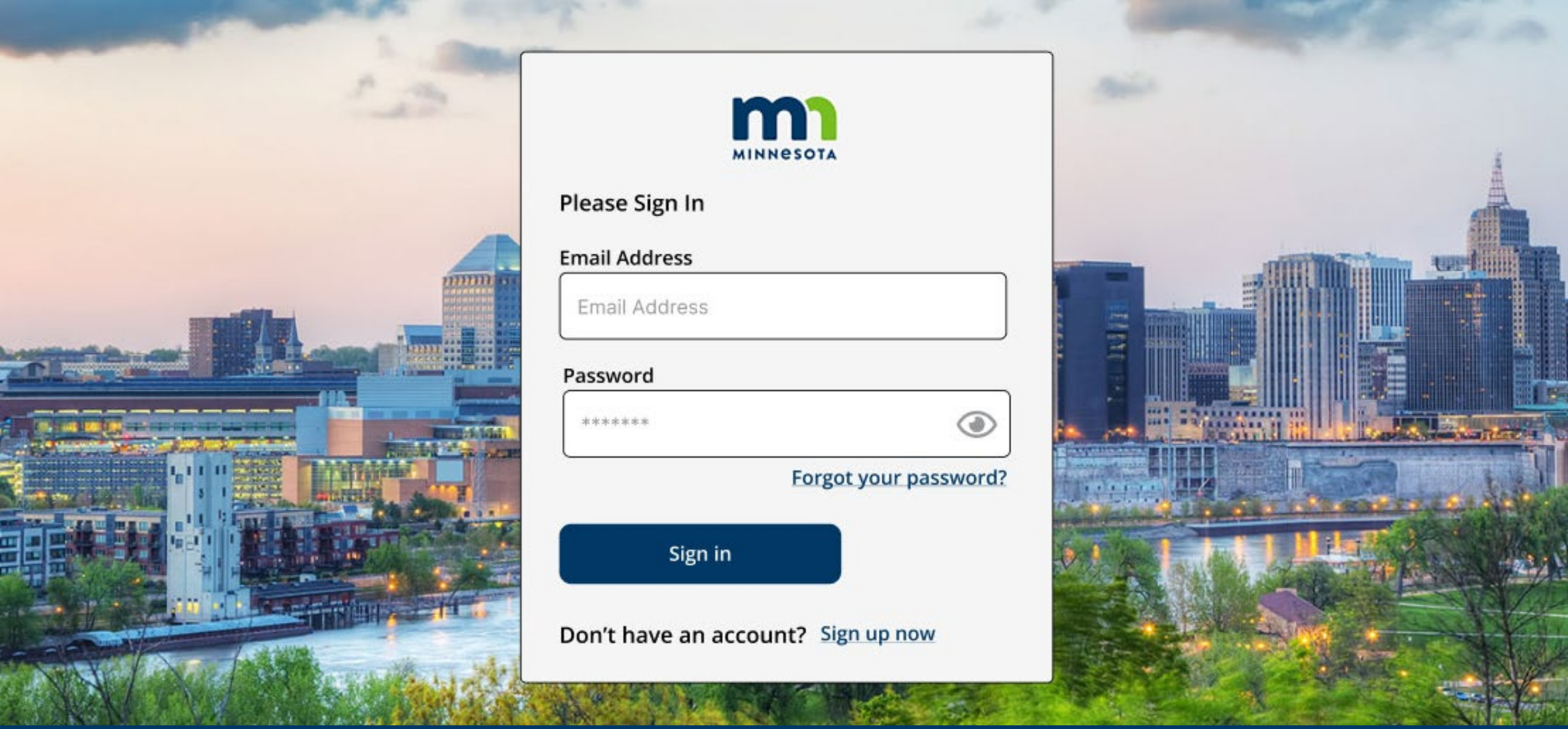
- Empowers constituents to control access.
- Provides single point-of-entry/portal to gain access to various applications.
- Increases compliance with continually evolving security policies and standards.
- Enhances reporting capabilities.

Benefits to Constituents

- Only need one set of credentials: one username and one password.
- One portal provides universal access to public-facing state services.
  - For example: Reserve a campsite, file taxes, complete a permit application.
- Adaptive AI will learn users' behavior to protect against fraud, bots, and account takeover.

Program Overview

- Received $6.2M in 2023.
- Investing in licensing and implementation services to build foundation for a modern, cloud-based IAM solution.
- Improving identity verification, risk mitigation, and access capabilities with automation.
- Equipping applications for a modern, standardized approach.

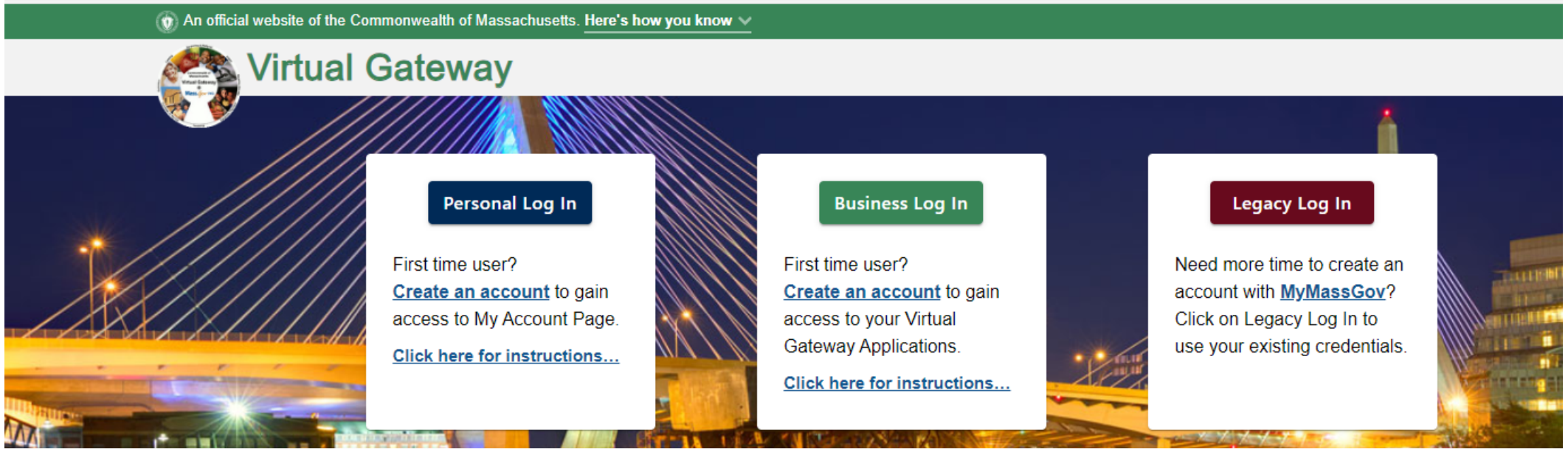


Building a Better Service

Building a Better Service: A New Name

Minnesota will align with other states use a similar approach, including:

- **Kansas:** KanAccess, www.kansas.gov/user/login
- **Pennsylvania:** Keystone Login, keystonelogin.pa.gov/Account/Login
- **Massachusetts: MyMassGov,** Mass.gov



Thank You!

John Israel | Chief Information Security Officer

john.israel@state.mn.us