Overview

• About Minnesota IT Services
• MNIT Cybersecurity Program
• Cybersecurity Threat Landscape
• MNIT Statewide Security Initiatives
• Infrastructure Investment and Jobs Act
Minnesota IT Services (MNIT)

Enable  
Deliver Value  
Protect
MNIT by the Numbers

- 114,777,986 Visits to state websites
- 11,708,461 Visits to DEED’s Unemployment Insurance websites
- 20,398,681 Visits to state websites for COVID-19 vaccine, testing, and information
- 4,271,774 Visits to MNsure websites
- 1,835 Number of security incidents resolved
- 2,435 Employees
- 2,080 Number of applications supported
- 545 Total projects tracked
- 10,000 Network devices supported
- 289 Number of websites we host and support
- 373,100 Service desk tickets across the executive branch
- 183,732 Tickets resolved the same day (49.25%)
- 952 Total resources on the Minnesota Geospatial Commons
- 102,169,512 Number of hits on the geospatial image server
- 4,739 Purchase request volume
In 2020, UI met unprecedented needs for over 1 million Minnesotans, paying out over $9.1B in claims. Over 47 million logins.

Unemployment Insurance changed a lot between 2019 and 2020:

• The amount paid in 2020 was 12.6 times larger than 2019.

• In 2019, UI did 4 quarterly builds. In 2020, we did 21 deployments.

• Even with all the changes, increased volume and expanded hours the system has only had 15 minutes of unplanned downtime.
COVID-19 Vaccine Technology Journey

- Vaccine Locator Map
- Vaccine Lottery Sign-Up for At Risk Individuals
- COVID-19 Vaccine Data Dashboard
- Vaccine Connector
- Vaccine Rewards Program
- Docket App
Minnesota Network for Enterprise Telecommunication (MNET)

MNET provides digital operations and connections for more than 375 non-executive partners.

Services:

- **WAN** - Connects over 1,700 locations in 300+ cities to MNET.
- **LAN** - Manages 1,200+ locations and support for 6,500 LAN and 2,300 WLAN devices.
- **Voice** - Supports 35,000 phones and 2,000 contact center agents in 55 contact centers.
- **Firewall** - Protects over 1,200 state office locations and the two main State data centers.
- **Conferencing** - Provides video and audio collaboration in more than 500 locations.
One of MNIT’s strategic plan goal is to bolster cybersecurity efforts. To do that, MNIT focuses on four pillars.
MNIT Security Operating Model

Enterprise Security Office (ESO)

- Governance, Risk, and Compliance (GRC)
- Secure Engineering and Architecture (SEA)
- Identity and Access Management (IAM)
- Threat and Vulnerability Management (TVMU)
- Digital Forensics and eDiscovery
- Security Operations Center (SOC)

Line of Business Teams

- DHS, MNsure
- General Government
- MDH, Health Licensing Boards
- DEED
- Revenue
- MnDOT, Commerce, PUC
- DPS, DOC, MDVA
Cybersecurity Threat Landscape

 Threat Groups 2021

- **Total Groups**: 2800+
- **FIN Groups** (2 Graduated): 13
  - Active FIN Groups
    - Groups From These Geolocations
      - Ukraine
      - Mexico
    - Groups Identified in 2021 (1141)
- **UNC Groups** (339): 51
  - Active UNC Groups
    - Groups From These Geolocations
      - China
      - Colombia
      - India
      - Iran
      - Latvia
      - Nigeria
      - North Korea
      - Russia
      - Slovenia
      - Switzerland
      - Slovakia
      - Turkey
      - Vietnam
- **APT Groups** (40*): 6
  - Active APT Groups
    - Groups From These Nation-States
      - China
      - Iran
      - Vietnam

*Source: Special Report Mandiant M-Trends 2022

*Mandiant tracks Advanced Persistent Threat (APT) groups 0–41. Over the years, APT 11 and APT 13 were merged into other groups and subsequently deprecated resulting in 40 APT groups actively tracked by Mandiant.
Top Targets of Cyber Threats in 2021

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>PERCENT OF INVESTIGATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business and Professional</td>
<td>14%</td>
</tr>
<tr>
<td>Financial</td>
<td>14%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>11%</td>
</tr>
<tr>
<td>Retail and Hospitality</td>
<td>10%</td>
</tr>
<tr>
<td>High Tech</td>
<td>9%</td>
</tr>
<tr>
<td>Government</td>
<td>9%</td>
</tr>
<tr>
<td>Transportation and Logistics</td>
<td>8%</td>
</tr>
<tr>
<td>Construction and Engineers</td>
<td>6%</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>4%</td>
</tr>
<tr>
<td>Education</td>
<td>4%</td>
</tr>
<tr>
<td>Energy</td>
<td>3%</td>
</tr>
<tr>
<td>Entertainment and Media</td>
<td>3%</td>
</tr>
<tr>
<td>Utilities</td>
<td>1%</td>
</tr>
<tr>
<td>Aerospace and Defense</td>
<td>1%</td>
</tr>
<tr>
<td>Agricultural and Forestry</td>
<td>1%</td>
</tr>
<tr>
<td>Nonprofit</td>
<td>1%</td>
</tr>
</tbody>
</table>

*Source: Special Report Mandiant M-Trends 2022*
On 24 February 2022, Viasat’s KA-SAT network experienced a multi-faceted and deliberate cyber-attack against its consumer-facing satellite broadband service.

While most users were unaffected by the incident, the cyber-attack did impact several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe.

They detected high volumes of focused, malicious traffic that came from several modems and/or associated customer premise equipment (CPE) physically located within Ukraine.

*Source: Viasat Overview and Incident Report [link]*
MNIT Statewide Security Initiative

- Endpoint Detection and Response
- Incident Response
- Threat Intelligence
- Advanced Log Collection / SIEM
- Vulnerability Management

SOC Cyber Navigator | Vulnerability Analyst
Compliance Support

Support and Resources
- MNIT SOC Engineers | MNIT SOC Analysts | MN Fusion Center | Federal Partners | Private Partners
Cybersecurity Grant Program for State, Local, Tribal Territorial Governments

- Infrastructure Investment and Jobs Act (IIJA)
  - Sec. 70611, State and Local Cybersecurity Improvements Act

- This could activate $17.932M for Minnesota in FY22-FY25.
  - FY22: $3,586
  - FY23: $7,173
  - FY24: $5,380
  - FY25: $1,793

- 80% of funding goes to local, tribal, and territorial governments (25% to rural areas based on census data).

- The Governor’s budget recommendations included a proposal to fund the state match for federal funds.
Cybersecurity Plan and Planning Committee

• Eligible entities submit a cybersecurity plan to Cybersecurity Infrastructure and Security Agency (CISA) that describes how they will protect against cybersecurity risks and threats to information systems owned or operated by state, local, or tribal governments.

• Cybersecurity plans are developed by cybersecurity planning committee and approved by the State CIO or State CISO.

• The planning committee shall:
  • Assist with developing and implementing the cybersecurity plan,
  • Approve the cybersecurity plan, and
  • Assist with determining effective funding priorities for the grant.
Representatives from:

- State
- Counties
- Cities
- Towns
- Institutions of public education
- Institutions of public health
- Tribal Nationals

- No less than half of the members will have professional cybersecurity or IT experience.
- It will also include, as appropriate, members from rural, suburban, and high-population jurisdictions.
1. Minnesota legislature debating whether to fund the state match to activate federal match.

2. Receive detailed guidance from CISA.

3. Activate the Minnesota Cybersecurity Planning Committee to align statewide plan and reporting criteria based on CISA guidance and requirements.

4. Submit grant application for Minnesota and develop procedure to manage execution of cybersecurity plan.
Thank You!

Rohit Tandon

Rohit.Tandon@state.mn.us