Report of the

STATE OF MINNESOTA BLUE RIBBON COUNCIL ON INFORMATION TECHNOLOGY

June 2020

This report of the Blue Ribbon Council on Information Technology proposes recommendations for improving the state of IT for Minnesotans, with background information and related considerations.


WEST
94

Contents

Letter from the Chair

June 30, 2020

Governor Tim Walz
Lt. Governor Peggy Flanagan
Speaker of the House Melissa Hortman
House Minority Leader Kurt Daudt
Senate Majority Leader Paul Gazelka
Senate Minority Leader Susan Kent
MNIT Commissioner Tarek Tomes

Cc:
Members of the Blue Ribbon Council on Information Technology

We are pleased to submit the final report of the Governor's Blue Ribbon Council on Information Technology.

Governor Walz issued Executive Order 19-02 and created the BRC-IT, engaging many of his key state agencies and adding state CIOs, county IT leaders and the Minnesota Association of Professional Employees (MAPE), to the mix. Governor Walz identified three subcommittees to address Cybersecurity, Data Privacy, and Modernization, and set the council to expire on June 30, 2020. Monthly meetings of the full council began in March 2019 and have continued through June 2020. In addition, each sub-committee has maintained a schedule of either monthly or bi-weekly meetings. Since its inception, three quarterly reports were published by the full BRC-IT, in June 2019, September 2019, and December 2019.

The BRC-IT structure and overall support allowed it to become much more influential and effective compared to its predecessor, the Technology Advisory Committee. There were three key items leading to this. First, the inclusion of more CIOs from Minnesota's leading companies was a huge improvement. Second, the Governor hired a new state CIO and gave him a clear mandate to work with and use the BRC-IT to help transform IT in the state. Third, including four legislators on the BRC-IT contributed to a richer, more well-rounded discussion.

The blend of private, public, county, union, and elected officials made for a perfect mix. Everyone agreed to listen to each other and to seek common ground. Council members agreed at the first meeting to reach consensus on each item that would appear in the report rather than vote, unless absolutely necessary. Happily, there weren't any votes. Members listened and worked to convince colleagues of their view. It was a bold gambit to achieve full consensus based on the BRC-IT's discussions, and it delivered.

As you read through this report, you will find a series of recommendations, a Playbook for effective state IT operations, and a view about how agencies using IT should be looking at their work and the IT services needed. Transforming IT does not just involve IT. It starts from knowing the required business outcome and using technology to help deliver services for the residents of the state. It is not just a one-time investment in a new application either. Ongoing funds for maintenance, operations, upgrades, and ultimately

replacement are key to long-term planning and funding. The recommendations highlight the importance of agency leadership in the success of IT, which is as important as an effective IT agency. For MNIT to be successful in leading and coordinating IT modernization, operations, and security it must take an expanded role as the centralized leader and coordinator of IT governance in collaboration with state agencies. Executive and legislative branch leaders need to prioritize investments needed to support this expanded role.

There are two other key items to consider in ensuring the success of IT in the state. Counties often are key members in the chain of implementation of state practices. A successful partnership between the state and the counties is required. The second piece is the IT worker in the state. Minnesota is blessed with many hardworking and dedicated IT workers, some in the central IT function at MNIT, and others based in the agencies – MNIT Partnering with MnDOT, for example. These professionals are key to our success now and in the future. Careful hiring, ongoing development and retention of strong performers will help MNIT and the agencies fulfill their missions.

I would be remiss not to call out the support that enabled the Council to do its work efficiently and effectively. When the membership of the BRC-IT was finalized, the chair recruited three additional volunteers from the private sector to act as writers for each of the subcommittees and the full council report. The addition and integration of these three has helped the council members focus their time on ideas and discussion versus writing and recording items for the report. In addition to the energy and enthusiasm of the three, the BRC-IT members have remarked quite often how these three have saved them countless hours. This is a best practice for sure. Many thanks to Amy Albus, John Klun, and Betsy Lulfs for their countless hours and tireless work.

The BRC-IT also benefited from its administrative support within MNIT. Many thanks to Taylor Mills, Michael Hainlin, Brandon Hirsch, and Deputy Commissioner Jon Eichten.

Should any of you or your members have questions about recommendations in the report, please let us know. We look forward to seeing the recommendations adopted.

Respectfully submitted,

Rick King
Chair, Blue Ribbon Council on Information Technology

Executive Summary

> *Up from 73% two years prior, a 2016 Accenture Study[1] revealed that 85% of citizens are "expecting the same or higher quality from government digital services as they do from commercial organizations."*

In the early days of the Walz administration, the state had some challenges with IT applications. To be fair, these issues were carried over from previous administrations, but this governor wanted them resolved. To do so, he first kicked off an exhaustive search for **a new state CIO**. Under the leadership of Kathy Tunheim, the state assembled a search committee, including many of the state's private and public IT leaders. The extensive search led to the hiring of **Tarek Tomes** as state CIO and Commissioner of MNIT.

Concurrently, Governor Walz issued **Executive Order 19-02**[2] and **created the BRC-IT**, engaging leaders at several of his key state agencies and adding state CIOs, county IT leaders, and MAPE voices as well. All selected BRC-IT members were assigned to one of three subcommittees: Cybersecurity, Data Management & Privacy, or Modernization. Monthly meetings of the full council began in March 2019, chaired by Rick King, executive vice president at Thomson Reuters, and have continued through June 2020. In addition, monthly or bi-weekly subcommittee meetings began in April 2019. The meetings have been a combination of **presentations** from subject-matter experts from the private sector, counties, and state agencies, and **working sessions** to discuss and prepare recommendations. Guest presenters are listed in Appendix D.

The **membership of the BRC-IT was key**. The addition of five CIOs from Minnesota companies helped transform the BRC-IT, bringing valuable ideas and advice from their corporate experiences. Also, the benefits from the addition of a new CIO for the state cannot be overstated by the BRC-IT. The new CIO was given the same mandate as the BRC-IT by the Governor, who really wanted things to improve. The CIO's passion for the work and improving IT was apparent from the start. His commitment to and collaboration with the BRC-IT have expedited improvements for MNIT and agencies.

In addition to the executive order creating the BRC-IT, legislation passed in March 2019 directed the Chair of the BRC-IT to lead an immediate review of MNLARS. Emergency funding for the project was tied to the findings of the report. The Independent Expert Review of MNLARS[3] was submitted by the Chair, one other BRC-IT member, and two additional individuals on May 1, 2019, and recommended replacement of the custom-built MNLARS with the purchase of a packaged software solution. This was a breakthrough after 10 years of

1 Accenture Consulting, "Accenture Public Service Pulse Survey: Digital government: Great expectations, untapped potential," https://www.accenture.com/t20160912t092658__w__/us-en/_acnmedia/pdf-30/accenture-digital-citizen-experience-pulse-survey-highlight.pdf (accessed May 24, 2020).

2 State of Minnesota, Executive Department, Executive Order 19-02, Establishing the Governor's Blue Ribbon Council on Information Technology, February 6, 2019, St. Paul, Minn., https://www.leg.state.mn.us/archive/execorders/19-02.pdf (accessed May 24, 2020).

3 Rick King et al., "Independent Expert Review of MNLARS," May 1, 2019, https://www.leg.state.mn.us/docs/2019/mandated/190649.pdf (accessed May 24, 2020).

challenges, and it led to a bipartisan solution with broad support from MNIT, Department of Public Safety, the Governor, the Legislature, and other stakeholders.

It was key for the state to honestly examine how it used technology and operated its IT services around the state. The BRC-IT addressed this immediately, hearing from agencies and counties about what was working and what was not. Many had serious needs. Others had best practices. We saw vastly different stages of maturity in planning and execution from agency to agency. We wanted to **identify best practices** and share them in our meetings. We wanted to help resolve the challenges in troubled projects.

The BRC-IT has published **three quarterly reports**, in June 2019, September 2019, and December 2019. This report reflects on the recommendations included in those reports[4] – the action already taken and the appropriate next steps – and includes new recommendations not previously presented. Both refined and new recommendations included here have been agreed upon unanimously by council members.

In this report, the BRC-IT is recommending the establishment of a **Modernization Framework**, which includes:

- **Identification of shared modernization principles.**
- **Creation of a Playbook** for collaboration between MNIT and agencies.[5]
- **Evaluation of the skills, leaders, and partners necessary and available** to aid modernization efforts.

A solid framework, with a set of principles, a playbook, and the people required for modernization, enables agencies, with support from MNIT, to establish a **Modernization Outlook** and enables MNIT to identify what changes must be made to the current **funding model** to speed up modernization, while ensuring due attention is paid to cybersecurity and to data management and privacy.

Parallel to the work of the BRC-IT, the **new state CIO** has been setting a course for improved IT services. In his first year, Commissioner Tomes led with a focus on building relationships and connections within MNIT and with all partners and stakeholders to improve the quality of service and increase efficiency.

He has also worked to increase transparency about MNIT's work with real-time availability of performance metrics. Cybersecurity has also been a priority from the start of his term, with a significant appropriation of dedicated cybersecurity investment and extra attention paid to recovery capabilities for critical applications and implementation of multi-factor authentication.

Modernization of IT services is a key theme, with focused discussion on modernizing applications, reinforcing data centers against physical and cyber-attacks while moving to the cloud where possible, extending and expanding security protections, and dealing with privacy issues.

The path to modernization calls for thoughtful planning when acquiring and building new applications. We need to think about when to **buy versus build**, and we must consider successes in other states. When we first introduce new

4 The recommendations included in the 2019 reports are listed in Appendix E.

5 Throughout this report, we use the term 'agency' as defined in Minnesota statute. Minnesota statute defines an agency as, "any state officer, board, commission, bureau, division, department, or tribunal, other than a judicial branch court and the Tax Court, having a statewide jurisdiction and authorized by law to make rules or to adjudicate cases." The word, "agency," also includes the Capitol Area Architectural and Planning Board. Minnesota Legislature, Office of the Revisor of Statutes, Minnesota Statutes, Section 14.02, https://www.revisor.mn.gov/statutes/cite/14.02.

technology, we need to **consider the entire lifecycle**, including acquisition, enhancement, upgrades, maintenance, operations, and even replacement. We need to think about **modernization of business processes**, too – and **must adapt business processes to standard software practices** rather than the reverse. We must also note the different **talents and skills needed** to manage operations, risk, and security in a cloud-based environment as compared to an on-premise data center environment, to procure the right solutions and to ensure business continuity.

In plotting the future experience, we must enable **effective and simple self-service for the end user**. So many of the state's transactions with citizens could be done by the citizens themselves using online functions or regional kiosks fit for the purpose.

None of this will happen without a **climate** in the state agencies and especially within MNIT that **embraces innovative change**, **transparency, and collaboration**. Embracing change is not just an internal mindset but also a willingness to reach out to others to seek best practices. The state must continue to reach out to its private sector but also look for states, like North Dakota, who have fully embraced a change agenda from the top down. Other states and localities might demonstrate best practices that Minnesota can deploy to advance IT practices.

As the BRC-IT was about to enter its last quarter before its final report, the world was hit with **Covid-19**. It was clear that many of the strategies used to "work from home" were thought through by IT and business leaders long before the pandemic came. The successful response to the unprecedented situation was evidence of thoughtful leadership, a changing culture, and the valuable skills of MNIT employees.

We recognize the forecasted impact of Covid-19 on the state budget and the temptation to reduce agency spending on technology. While reduced IT spending is a consideration, reductions must be considered carefully. It is this scenario that increases risk by delaying maintenance investments and updates for state IT systems that are needed to safeguard state data assets from cybersecurity attacks and disruption of services to Minnesotans. Moreover, **modernization of IT is an investment in the infrastructure of the state that can achieve higher quality services and more efficient operations**. Given the expected budget shortfall, executive and legislative branch leaders should consult with state leader members of the BRC-IT to prioritize our recommendations where funding is needed.

List of Recommendations

All the following recommendations appear throughout the report, in line and with relevant context. They are listed here, without context, for easy reference. The BRC-IT views all the recommendations as important for successful modernization and advises agency and MNIT leaders to discuss them together and prioritize them where resources are needed. We recognize this may extend the timeline for implementing the recommendations, but hope they are all given due attention and consideration. **Plans or progress reports for all recommendations should be presented to the BRC-IT by the end of 2020.** Those requiring legislative action should be afforded greater urgency and should be presented to the BRC-IT for discussion as soon as possible, but no later than November 1st, 2020.

Section 2 | Blue Ribbon Council on Information Technology

1. **The Minnesota Legislature should amend the Minnesota statute authorizing the Technology Advisory Committee and rename the committee the Technology Advisory Council, with membership and mission replaced with that of the current BRC-IT.**

Section 3 | Modernization Principles and a Modernization Review Board

2. **MNIT should involve agency and technology leaders in the creation of business and technology modernization principles and establish a review process to ensure that the principles evolve as needed.**

3. **MNIT should establish and host a Modernization Review Board (MRB) that includes key agency leaders to review the adoption of modernization review practices for large-scale or critical technology initiatives across the state.**

Section 4 | Modernization Playbook

4. **Agencies should evaluate and simplify business processes and rules before building, replacing, or procuring new systems and make recommendations to the Legislature regarding modifications to laws and regulations.**

5. **MNIT and the Department of Administration should develop and implement a plan to ensure that agencies understand and use their authority and ability to engage more fully with vendors before a final vendor is selected.**

6. MNIT should build capacity within the procurement unit to develop procurement strategies and support acquisitions for IT modernization projects.

7. MNIT and the Department of Administration should jointly assess the current vendor risk through a structured process and security framework for contract management and risk prioritization.

8. MNIT should provide education for agencies on the IT security risk assessment process and partner with agencies to assess, manage, prioritize, and communicate any risks encountered during the process.

9. Agencies should conduct a privacy impact assessment for all information technology projects as part of the project initiation process.

10. MNIT should establish a plan for real-time access to project and portfolio management reporting that ensures effective communication with all stakeholders.

11. MNIT, working with state agency partners, should create education and training to introduce the Modernization Playbook to all MNIT staff and agency leaders and draft a plan to drive, govern, and measure adoption and acceptance of the Playbook.

Section 5 | People Enabling a Modernization Vision

12. State agencies should include the CBTOs in the agencies' various leadership teams and include them in the highest appropriate level of leadership meetings and strategy planning.

13. The executive branch should establish a chief privacy officer position to support state practices on data privacy and sharing.

14. MNIT should establish an awareness campaign and a cybersecurity education and training program that can be made available to legislators and others in state government.

15. MMB should assess the feasibility of a Skilled Professional Program, identifying the appropriate authority for the program and whether statutory changes are required, and then present their findings to the BRC-IT.

16. MNIT should explore the feasibility and, if appropriate, outline a plan for creation of a public/private partnership for cybersecurity.

17. The Legislature should create two new legislative coordinating committees – one for cybersecurity and one for technology.

18. MNIT and state agencies should include other governmental units (including MNCITLA) and tribal governments as partners at project launch and include an assessment of their data needs and challenges in establishment of data privacy and management policy.

Section 6 | Enterprise Strategy for Modernization

19. MNIT should collaborate with agencies on the development of a 10-year Outlook for Business Modernization and the related 5-year plan for technology modernization.

20. MNIT should convene a working group of MNIT and agency staff to present a plan to catalog all data managed by the state, establish a metadata framework that enables data sharing and system interoperability, and identify guidelines for retaining and purging data.

Section 7 | Funding

21. Agency and MNIT leaders should review the Modernization Playbook and identify strengths, weaknesses, and capability gaps in the current staffing, processes and technology for each agency and submit to MMB, for consideration by the Governor through the state budget development process, the changes to current funding needed to address these gaps.

22. Cybersecurity protection should be declared critical infrastructure to allow for alternative funding capabilities, protection of operations, and expeditious responses to emergencies.

23. The Legislature should ensure that the state has long-term, consistent, predictable, and appropriate funding for cybersecurity operations, based on a percentage of the total state IT budget.

24. MNIT should expand the disaster recovery roadmap to include all Priority 1 and Priority 2 applications and support additional funding to complete cloud-focused recovery capabilities for stability, data protection, and resiliency for critical systems and applications.

Section 1

Section 1

Blue Ribbon Council on Information Technology

History of the Blue Ribbon Council on Information Technology (BRC-IT)

The Minnesota State Legislature created a Technology Advisory Committee (TAC) in 2011 to advise Minnesota's Chief Information Officer on technology strategy and management. The law[6] called for appointment of nine members by the Governor including one representative each from the private sector, the union, and the Association of Minnesota Counties, in addition to representatives from state executive branch agencies.

As part of a legislatively mandated comprehensive review[7] of executive branch advisory groups in 2013, the Legislative Commission on Planning and Fiscal Policy (LCPFP) recommended that TAC continue, subject to biennial reviews by the LCPFP.

Since 2011, the TAC has advised the state CIO on the development and implementation of the following:

- State IT Strategic Plan.
- Critical IT Initiatives.
- IT Architecture Standards.
- Identification of Agency Business and Technical Needs.
- Strategic IT Portfolio Management.
- Project Prioritization.
- Investment Decisions.
- Performance Measures and Fees for Agency Service Agreements.
- Management of State Enterprise Technology Revolving Fund.
- Efficient and Effective Operation of MNIT.

According to the 2019 Evaluation Report of the Office of Minnesota Information Technology Services by the Office of the Legislative Auditor, the TAC's advisory contribution to MNIT was limited. Specifically, the report cited infrequent meetings as a reason for the limited impact. The committee met five times in 2012, and 11 times over the following six years. Chair King has served on the TAC since it started in 2011.

On February 6, 2019, by Executive Order 19-02, Governor Walz established the Blue Ribbon Council on Information Technology (BRC-IT) as an **expansion of the TAC** with its active nine members, six additional members appointed with private-sector or public-sector IT experience, and four

6 The full text of the law creating the TAC can be found in Appendix A and at https://www.revisor.mn.gov/statutes/cite/16E.036.

7 State of Minnesota, Legislative Commission on Planning and Fiscal Policy (LCPFP), *Executive Branch Advisor Groups Recommendations (December 18, 2013), St. Paul, Minn.,* https://www.commissions.leg.state.mn.us/lcpfp/advisory_groups/LCPFPfinalreport12182013.pdf (accessed May 24, 2020).

ex officio non-voting members selected by the majority and minority leaders of the House and Senate. Appendix C lists the members of the BRC-IT, along with their subcommittee assignments.

The executive order stated that "Minnesotans expect reliable, secure, and accurate information technology services when they interact with the state" and noted that "the Blue Ribbon Council on Information Technology was created to **ensure the people of Minnesota have access to high-quality, dependable services**." Governor Walz identified three subcommittees to address Cybersecurity, Data Privacy, and Modernization, and set the council to expire on June 30, 2020. He appointed Rick King, Executive Vice President of Thomson Reuters, to Chair the BRC-IT.

More specifically, the BRC-IT was tasked with the following:

- Review and clarify the role of MNIT.
- Serve as a consultant for MNIT and state agencies.
- Review legislation, policies and practices related to IT.

As a first order of business for the BRC-IT, Governor Walz requested an **immediate review of MNLARS.** The Independent Expert Review of MNLARS was submitted on May 1, 2019 and recommended replacement of the custom-built MNLARS with the purchase of a packaged software solution.

This was a very important milestone in the troubled MNLARS project, for many reasons. First, many believed it to be a fully transparent report about MNLARS following years of acrimony. The Governor and legislative leadership wanted a fair, full and transparent recommendation. Second, the ultimate outcome – recommending the selection of a third-party software provider – reminded us that as much as we always like to think what we are doing is unique, it rarely is. In the case of FAST, the selected vendor, they had previously implemented their driver and vehicle solutions in eight other states, learning and improving the solution each time then providing proven results and the benefit of collective intelligence to Minnesota residents. The principle of buying before building whenever possible is one of the key lessons learned from

Top row: Tewodros "Teddy" Bekele, Land O'Lakes; Tom Butterfield, TCF Bank; Mike McCullough, National Marrow Donor Program; Renee Heinbuch, Washington County; Jason Lenz, Lyon County; Laurie Martinson, MN Dept. of Natural Resources, Theresa Wise, formerly Delta/NW Airlines.

Bottom row: Lee Ho, MN Dept. of Revenue; Eric Hallstrom, MN Management and Budget; Margaret Anderson Kelliher, MN Dept. of Transportation; Rick King, Thomson Reuters; Tarek Tomes, MNIT; Rep. Kristin Bahner; Sen. Melissa Wiklund; Rep. Jim Nash.

Not pictured: Kasandra Church, MN Assoc. of Professional Employees; Steve Grove, MN Dept. of Employment and Economic Development; Chuck Johnson, MN Dept. of Human Services; Sen. Mark Koran; Nancy Lyons, Clockwork.

the MNLARS project. This lesson guides us for the future.

Separately from the MNLARS review, the BRC-IT held 18 monthly full council meetings, with separate subcommittee meetings to gather and review information specific to their subcommittee assignments and bring recommendations to the full council.

The BRC-IT structure and overall support allowed it to become influential and effective. **Three key items** contributed to this improvement:

- The inclusion of more CIOs from Minnesota's leading companies.
- The Governor's mandate to the new state CIO to work with and use the BRC-IT to help transform IT in the state. The CIO took this to heart and has done much to improve the IT environment in the state.
- The inclusion of the four legislators.

The **Membership of the BRC-IT** was key. The addition of five CIOs from Minnesota companies helped transform the BRC-IT, adding new ideas and advice from the private sector. These IT leaders have undergone cybersecurity, recruiting, modernization and privacy challenges at their own companies and brought those outlooks to the BRC-IT. Although the Governor selected five in the end, more than four times as many applied to be part of the council. They paired very well with the six agency heads already on board and broadened the perspective of the group.

The benefits from the addition of a **new state CIO** cannot be overstated by the BRC-IT. His willingness to embrace the Governor's mandate to work with the BRC-IT also made a huge difference in the outcome. Even before his official first day in his new CIO position, he met with the BRC-IT to pledge his full support, as well as that of his agency, Minnesota IT Services (MNIT). From the start of his tenure, the BRC-IT was pleased to see a clear drive for change and improvement in relationships with the various state agencies MNIT serves.

Finally, the appointment of four legislators, one from each chamber and each party, was a critical element. They provided sharp focus and practicality in terms of steps toward formalization of recommendations, especially those that require statutory changes.

The BRC-IT was a perfect combination of state and local and private and public representatives, all with a commitment to improving the state of IT for Minnesota.

Three quarterly reports were published by the council, one in June 2019[8], one in September 2019[9], and one in December 2019[10]. The members of the BRC-IT provided input for and approved all recommendations contained in the quarterly reports, as well as the recommendations contained in this final report.

---

8 State of Minnesota, Blue Ribbon Council on IT, *June 2019 Quarterly Report, June 2019, St. Paul, Minn.,* https://www.leg.state.mn.us/archive/execorders/19-02.pdf (accessed May 24, 2020).

9 State of Minnesota, Blue Ribbon Council on IT, *September 2019 Quarterly Report, September 2019, St. Paul, Minn.,* https://www.leg.state.mn.us/docs/2019/other/191135.pdf (accessed May 24, 2020).

10 State of Minnesota, Blue Ribbon Council on IT, *December 2019 Quarterly Report, December 2019, St. Paul, Minn.,* https://www.leg.state.mn.us/docs/2020/other/200247.pdf accessed May 24, 2020.

Technology Advisory Council

The BRC-IT and the Technology Advisory Committee (TAC) before it shared similar objectives to advance an effective and strategic approach to information technology services. The BRC-IT, while limited in duration and narrow in scope, offered intensive focus and dedication to actionable progress. The TAC, while historically limited in its impact due to infrequent meetings, carried the benefit of its evergreen status through Minnesota statute.

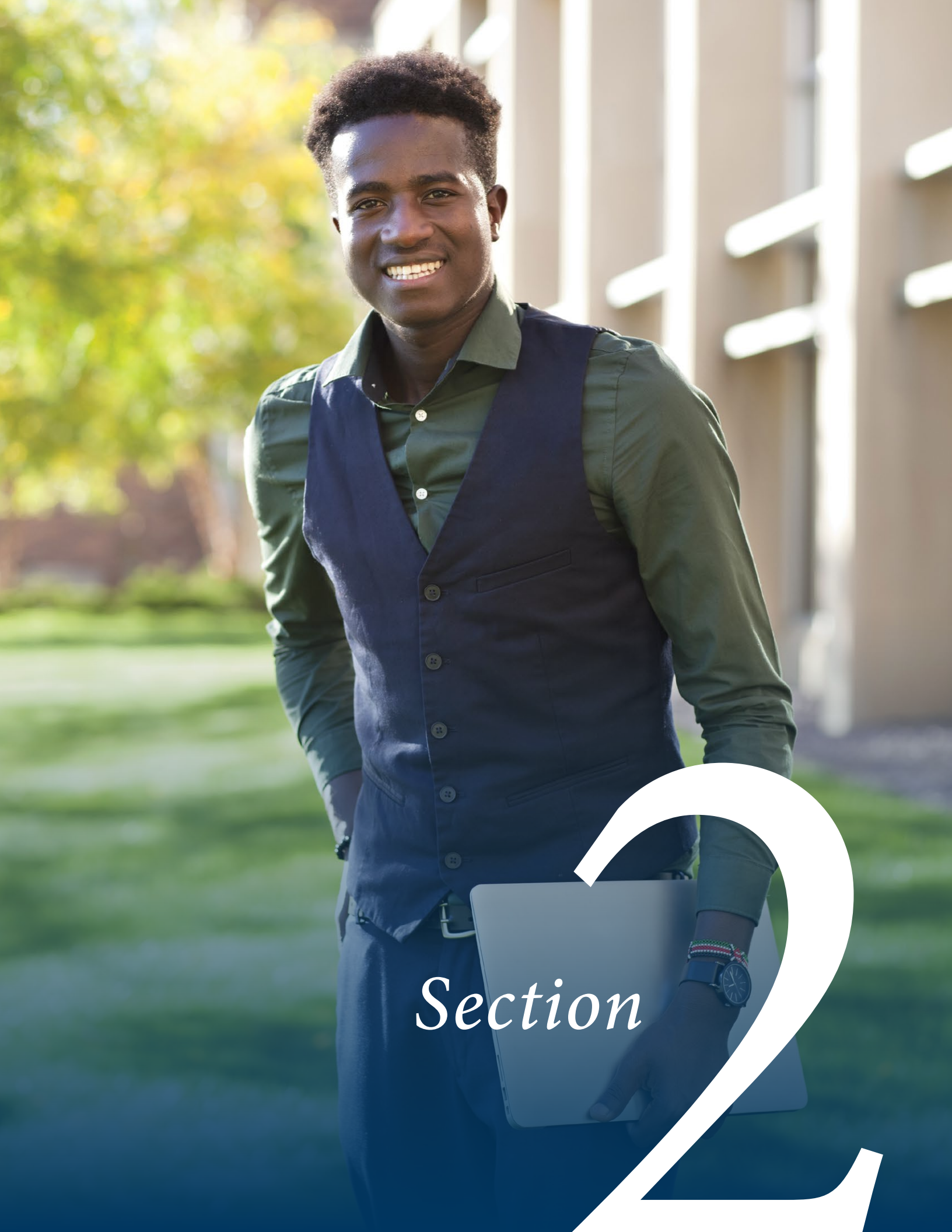
Recognizing the limitations of the TAC cited in the OLA report, the BRC-IT recommended legislation to capture the advantages of both bodies by an amendment to the statute authorizing the Technology Advisory Committee. In its September 2019 report, the BRC-IT recommended the Technology Advisory Committee be replaced by the current BRC-IT, specifying the following modifications to the existing statute:

- Include further collaboration with Native American tribal governments.
- Review and clarify the role of MNIT.
- Serve as a consultant for MNIT and state agencies.
- Review legislation, policies, and practices related to IT.

The new body has the evident advantage of retaining the knowledge and expertise of the existing members of the TAC, while adding the insight and expertise of new members with private- and public-sector experience, as well as the guidance of ex officio members. The legislation allows the state to recognize the benefits of this dedicated group on an ongoing basis. House File 4527[11] introduced in the 2020 legislative session contains changes to the statute reflecting the BRC-IT's recommendations. It also recommended the new body be named the Technology Advisory Council.

1. **The Minnesota Legislature should amend the Minnesota statute authorizing the Technology Advisory Committee and rename the committee the Technology Advisory Council, with membership and mission replaced with that of the current BRC-IT.**

11 The full text of HF4527 can be found in Appendix F and at https://www.revisor.mn.gov/bills/bill.php?f=HF4527&y=2020&ssn=0&b=house.



Section 2

Section 2

IT Services for the State of Minnesota

Introduction

Three events in recent Minnesota history serve as highlights of IT services for the state. They pinpoint areas that required correction, areas for continued improvement, and evidence of strength and promise:

- The Minnesota Licensing and Registration System (MNLARS) software rollout with significant deficiencies in 2017.
- The ransomware attack on the Minnesota Department of Corrections in 2019.
- The state's response to the Covid-19 (Coronavirus) challenge in early 2020.

MNLARS

The MNLARS event illustrates challenges faced with the launch of a significant software development project amid shifting agency-specific roles and authority within IT. The Office of the Legislative Auditor's report[12] on the event concluded that the MNLARS problems resulted from a lack of oversight by both the Department of Public Safety (DPS) and the Office of Minnesota Information Technology Services (MNIT). The report, published in February 2019, stated the following about MNIT:

> "The consolidation of state government information technology services into a single agency (MNIT)—which was mandated by 2011 legislation—remains a work in progress today."
>
> —OLA Report, Page 22

The OLA identified that, as part of completing IT consolidation, MNIT should strengthen its oversight of agency-based software development projects such as MNLARS and address the "lack of clarity about the respective roles of MNIT and state agencies in agency-based software projects." (Page 64)

Department of Corrections Ransomware Event

In contrast, the state's response to a ransomware event that affected the Minnesota Department of Corrections (DOC) in 2019 the Covid-19 event of 2020 exemplified the progress MNIT has made in recent years. The BRC-IT's tenure coincided with these events, and preliminary indicators suggest successful responses.

12 State of Minnesota, Office of the Legislative Auditor, Factors That Contributed to MNLARS Problems, St. Paul, Minn., https://www.auditor.leg.state.mn.us/sreview/mnlarsfactors.pdf (accessed June 24, 2020).

Lessons learned from previous challenges, as well as MNIT's access to a group of advisors with deep understanding and strong relationships due to their participation in BRC-IT, put the state in a good position to address both challenges. The unprecedented nature and broad impact of the Covid-19 pandemic response, in particular, tested the state. It included the need to rapidly transition a large portion of the state's workforce to a work-from-home environment, restructure the delivery of services to Minnesotans, and accommodate ballooning service needs—all in a short period of time.

In October 2019, the Minnesota IT Services (MNIT) security team identified and addressed a ransomware infection impacting the Minnesota Department of Corrections (DOC) Stillwater and Oak Park Heights correctional facilities.

After initial detection, the cyber incident response team was mobilized to take the affected computers, servers, and networks offline for containment and rebuild. While the DOC's local user devices and some agency applications were taken offline as a precaution, the correctional facilities' security systems and cameras were not impacted by the malware.

As DOC learned of the malware infection and assessed impact, they activated their facility continuity of operations plans, which remained in effect until all IT resources were fully restored in under a week. Because of the swift actions of MNIT professionals and the preparedness of DOC in their continuity of operations procedures, there was only a short period of efficiency lost during the cyber event, and Stillwater and Oak Park Heights correctional facilities continued to safely operate.

Covid-19 Response

The Coronavirus (Covid-19) pandemic put to test systems and processes throughout the world, including Minnesota. In March and April of 2020, Governor Walz issued multiple executive orders requiring closures and imposing stay-at-home orders. These orders had significant impact on state operations in terms of delivery of services, revenue adjustments, and rapid modifications to the State of Minnesota's own workforce to quickly deploy work-from-home capabilities in order to continue services with minimal disruptions.

Technology is at the center of enabling workforce and cultural shifts like these. It is also critical for delivery of the services that the people of Minnesota rely upon. MNIT acted quickly to provide access to critical services and expand and enhance teleworking capabilities for state employees. MNIT and state technology are evolving not just the teleworking capabilities of the State, but also the collaborative, coordinative capabilities to connect Minnesota to a better government.

The following are among the highlights of this unprecedented effort:

- Rapid transition of a workforce of 35,000+ employees to a majority work-from-home environment, which included rapidly expanding VPN capacity and expediting deployment of over 1,500 laptops.
- Uncompromising commitment to cybersecurity by ensuring continued adoption of multi-factor authentication through enhanced support and communication amid rapidly changing circumstances.
- Ensuring that Minnesota's Unemployment Insurance site (uimn.org) could support unprecedented numbers of applications (over 750,00) and incorporating state and federal changes to benefits and eligibility for unemployment insurance.

- Using technology solutions to address the fundamental challenges of the event itself. For example, using cell phone app data to measure movement and contact, and implementing virtual health screening applications to reduce worksite risks and spread of the virus.
- Continued commitment to ensuring that state business partners received the technical support they needed in order to serve Minnesotans by adopting innovative solutions and staffing reassignments. Technical support call volumes increased by as much as 450% and peaked at over 1,100 calls per day, versus the standard average of 200 calls per day.
- MNIT's communications team and website development team supported the Governor's office with developing Minnesota COVID-19 response portal providing access to over 4,000 pages of information related to the Coronavirus pandemic and Stay-at-Home and Stay Safe MN guidelines.
- A knowledge management chat bot was implemented on the COVID-19 portal to provide quick-access to the wealth of information available.

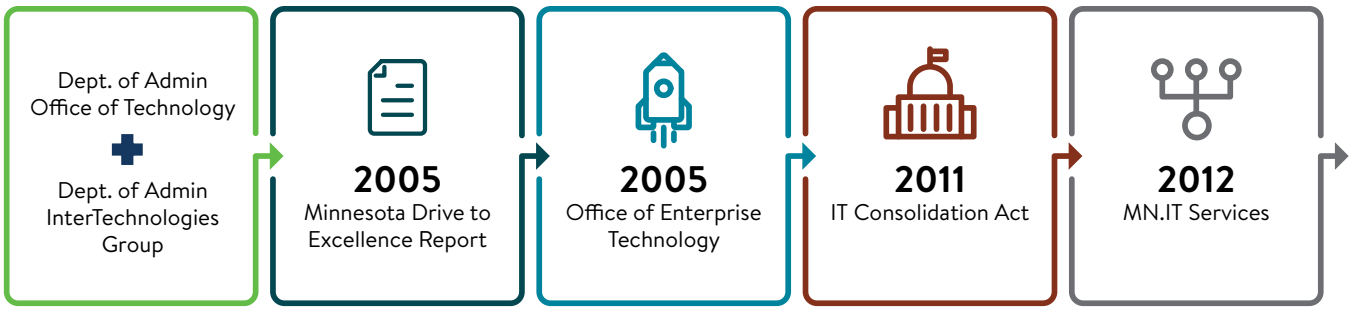
Importantly, Commissioner Tomes noted that the state's consolidated organizational structure for IT operations enabled the fleet-footed response to the event. Deployment of routers to homes, as well as the enterprise approach to VPN desktop enablement, worked well, and the consolidation of operational staff made for easier communication of safety-related guidance and personal protective equipment acquisition and distribution.

According to Commissioner Tomes, Minnesota's response to the unemployment challenge was one of the most effective in the United States. He offered as evidence the fact that Minnesota was the first to distribute the $600 supplemental unemployment benefit after it was approved by the federal government. Additionally, while state unemployment systems have highlighted the need for ongoing innovation amidst performance constraints, Minnesota's system has continued to accept and process applications while record-breaking numbers of applications are received.

> "In many cases, when things are approved, we're among the first to implement."
>
> —Commissioner Tomes

Furthermore, Commissioner Tomes noted that the event has fostered an environment of collaboration with county IT directors and other public- and private-sector partners. In this unprecedented situation, Minnesota again proved itself a community of action-oriented volunteers, willing to help wherever possible. Companies large and small have pitched in to assist.

This is all a result of many changes, large and small, to IT services over the last 15 years.



History of IT Services

The current iteration of IT services, with MNIT in the forefront, dates back to the actions of the 2011 Legislature[13]. The 2011 consolidation was the culmination of more than a decade of progress and decision-making in that direction. As early as 1996, Governor Arne Carlson issued an executive order establishing an Office of Technology Coordination specifically for education-related technologies. The Legislature created the Office of Technology in 1997, later placing it under the Commissioner of Administration's supervision. The Legislature combined the Department of Administration's Office of Technology and InterTechnologies Group to create the Office of Enterprise Technology (OET) in 2005. The OET focused on completing an enterprise email system, consolidating multiple systems into one – and delivering a limited set of shared infrastructure services such as wide-area network and mainframe services.

The Legislature enacted legislation to consolidate IT services within one agency in 2011 and changed the name from OET to MNIT in 2013. The Legislature also clarified in 2013 that the head of MNIT is both a commissioner and the state's chief information officer (CIO). It has centralized and distributed staff, with some dedicated to MNIT's enterprise services and many other MNIT employees working alongside their business partners embedded in state agencies. The **timeline for the consolidation of IT Services** can be found in Appendix G.

While almost all states have **consolidated IT** to some degree, the approach varies greatly from state to state. IT consolidation in many states is focused solely on the consolidation of infrastructure services, while a small number of states have implemented a full consolidation where all IT services are centrally delivered, and all state IT staff work for a single agency or department. Minnesota's approach to the 2011 legislative mandate reflects a hybrid approach.

In Minnesota, all state IT staff, with the exception of a handful of agencies explicitly exempt from the law such as the Campaign Finance Board and Minnesota Lottery, are MNIT employees. However, from a service delivery standpoint, MNIT employs a **hybrid approach** that combines a centralized service delivery model for an expanded set of commodity-type services (hosting, workstation management, service desk, wide area and local voice and data networks) with a decentralized approach to services such as application development and support. The decentralized approach to application support reflects a recognition that these roles require in-depth knowledge of unique business processes that exist across the state's executive branch agencies, boards, councils and commissions. This avoids the

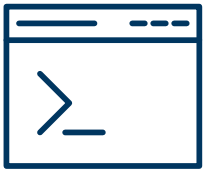
13 Laws of Minnesota 2011, First Special Session, Chapter 10, art. 10, art 4, codified as Minnesota Statutes 2011, 16B.99, 16E.016, 16E.036, 16E.04, and 16E.145.

common problems found in a "one size fits all" environment where services do not fully meet agency needs, but it creates the challenges of managing the costs of developing and maintaining highly customized applications and services.

In its February 2019 report, the Office of the Legislative Auditor found that "MNIT has limited central oversight of agency-specific services, so this oversight continues to be managed largely on an agency-by-agency basis."[14] MNIT has worked to **strengthen this central oversight capability** through the work of its Enterprise Portfolio Management Office, requiring enterprise-wide reporting on the status of agency-based IT projects and use of an IT Project Risk Management Master Contract program for the execution of external project risk assessments and audits for major IT projects. In addition, MNIT has established an enterprise oversight process where a team of senior MNIT leaders perform regular reviews of the status, risks, and challenges facing a select group of major IT projects that are large in scope and budget or particularly high-impact. Finally, in collaboration with the Governor's office, MNIT developed an Executive Go Live Communication Process supported by agency business leaders to elevate effective situational awareness of pending application launches, or go-lives, to allow senior leaders time to weigh-in on critical decisions and provide assistance as needed. This process fosters collaboration and an overall sense of shared ownership to reduce the risk of unsuccessful application launches.

Agency leaders outside of MNIT have expressed mixed opinions about the overall benefit of consolidated services. Among the additional challenges outlined by the 2019 OLA report on MNIT is a lack of clarity of the roles and responsibilities of MNIT and the agencies it serves. In particular, the report cites a lack of role clarity regarding software development, a gap that was particularly illuminated in the MNLARS project. On the other hand, the 2019 OLA Report on MNIT cites the consolidation as a contributing factor in valuable advancements in IT security. IT finance outcomes proved to be undetermined at the time of the report.

2,400+
People employed by MNIT



2,800+
Applications supported

350+
Active IT projects

5.5 million
Minnesotans whose private data is secured

14 State of Minnesota, Office of the Legislative Auditor, Office of Minnesota Information Technology Services (MNIT) 2019 Evaluation Report, St. Paul, Minn., Pg. 27, https://www.auditor.leg.state.mn.us/ped/pedrep/mnitservices.pdf (accessed June 10, 2020).

MNIT Today

In addition to ongoing IT service delivery for the executive branch, MNIT sets IT strategy, direction, policies, and standards for enterprise IT leadership and planning. The agency's growing set of responsibilities is evident in statistics published in its 2019 annual report. While the consolidation is complete with all IT resources reporting under a single agency, **service maturity is an ongoing process** to ensure efficient and effective delivery of services to the state and all Minnesotans.

The annual report calls out the **new leadership** under the direction of Commissioner Tarek Tomes and highlights IT success stories across the enterprise. It also outlines a tactical plan[15] aimed at bringing people, processes, and technology together to deliver greater value from public services to all Minnesotans. The plan envisions secure and modern technology systems that are built on reimagined relationships between MNIT, state agencies, and Minnesotans. The BRC-IT is a key partner in this effort. The report specifically cites the work and perspectives of the BRC-IT and Commissioner Tomes' cooperation with the organization.

Over the course of the BRC-IT work, the council's state agency members relayed that agencies are increasingly embracing the hybrid, federated model for IT governance and leadership. This has particularly been the case as agencies understand the critical role that they will play as business leaders in a consolidated model - setting the strategic direction and priorities for their business units and the unique applications that support their operations.

New Leadership of Commissioner Tarek Tomes

Commissioner Tomes began his tenure as MNIT Commissioner with a focus on building relationships – seeking to exemplify the role that technologists can play throughout government in building connections across agency lines, between IT and business teams, across levels of state and local government, and ultimately between Minnesotans and their government. He organized an in-person, cross-agency leadership event entitled "Reimagining the Relationship" that examined the role of MNIT as a business partner versus service provider, and brought in experts in human-centered design to facilitate an executive leadership-level conversation about how to strengthen the business-IT relationship and leverage that relationship to innovate and improve government service delivery. Commissioner Tomes and his team refer to this work as building a **Connected Culture** – a culture where the silos that have traditionally separated the work of government are overcome to better serve Minnesotans and improve government efficiency and effectiveness.

Commissioner Tomes also worked in his first year to increase the **transparency of MNIT's work** to its business partners and stakeholders, instituting a cadence of quarterly public reports to provide data-focused updates on the status of projects, initiatives, and services. He also added Chief Technology Officer Jeff Nyberg to his leadership team, whom he tasked with raising the bar of service maturity for MNIT's enterprise service teams by orienting their work around a set of performance metrics that can be monitored in real-time through data visualization dashboards. This shift to data-driven management was critical as MNIT responded to the demands of COVID-19 – rapidly responding to the IT needs of thousands of state employees as they shifted

15 Appendix H illustrates MNIT's 12-month tactical plan.

to telework, managing unprecedented volumes of transactions on the state's unemployment insurance system, managing spikes of traffic to state websites as major announcements occurred, and ensuring secure, reliable network access for tens of thousands of state employees working remotely. MNIT also made strides to improve the transparency of its financials by developing and making available to agency leaders the Athena Dashboard, which enables agencies to make more informed decisions and better manage their costs.

Several major projects also reached important milestones during the first year of the new commissioner's tenure and were reviewed through the Executive Go Live Communications Process, including:

- The stabilization of the MNLARS system and shift to implementation of a packaged software solution for vehicle services.
- An upgrade of SWIFT – the state's PeopleSoft-based online financial, procurement, and reporting system.
- Implementation of a mobile, cloud-based scheduling and timekeeping system for Minnesota veterans homes.
- Development of the MnDOT Identity Manager which automated personnel information updates for MnDOT's large number of full-time and part-time staff, as well as contractors and seasonal workers, eliminating manual, redundant processes to increase productivity.

Commissioner Tomes also made **cybersecurity** – in particular, responding to the threats posed by ransomware - a focus of his first year as State CIO. He issued a directive requiring enterprise and agency-based MNIT teams to assess the capability of meeting recovery time objectives for the state's most critical applications, ensuring those applications could be recovered from backup in the event of a ransomware attack on state systems to ensure the continuity of services upon which public health and safety rely. He also successfully advocated at the Minnesota Legislature for the first increase in dedicated cybersecurity appropriations in over a decade, resulting in a $5 million increase in base funding. Moreover, he made the implementation of Multi-Factor Authentication (MFA) a top priority of his first year in office, setting May 1, 2020 as a target date for completing implementation for the executive branch enterprise. MNIT maintained this focus on MFA implementation as tens of thousands of state employees shifted from in-office work to telework, resulting in over 96% adoption by the May 1 deadline.

Cybersecurity

Protecting data for 5.5 million Minnesotans and 2,800+ applications against external and internal threats is a top priority for the state.[16] As attacks are becoming more sophisticated and common, building security into every system and application is imperative. This requires funding and forethought.

Hackers gain entry to IT systems through various methods, some of the more well-known are phishing emails where the recipient provides credentials opening the door to the IT systems, infected email attachments, access through third-party service providers, infiltration of networks and servers, and installation of malware – to name a few. This intrusion severely impacts services and can take weeks to repair, significant expense for the purchase and deployment of new systems, and considerable resource deployment for forensic analysis and detection.

Results of hackers successfully infiltrating systems include issues like: knocking out online systems, email, phones, and water utility pump stations; loss or delay of revenue from sources such as fines, property taxes, and real-estate fees; computer

16 One of the MNIT's Top Priorities is to 'Secure the State.' More detail about this priority is available in Appendix H.

screens at a 911 dispatch center going dark forcing emergency dispatchers to take notes by hand and rely on printed maps of the county and paper logs to keep track of emergency responders in the field; and schools couldn't access data about students' medications or allergies to name a few. The list of representative cybersecurity incidents listed in Appendix N, though not exhaustive, gives an overview of systems that were impacted in 2019 ransomware attacks.

The infrastructure that protects national, state, and local elections is also critical to secure and protect. The state plays a vital role in collaborating with statewide jurisdictions as well as the federal Department of Homeland Security in ensuring confidentiality and accuracy of fair and free elections. Minnesota has one of the highest voting rates in the country. In the 2016 election Minnesota had a 74.8% voter turnout rate, the number one ranking in the country, and the state consistently ranks high in all elections as shown by Ballotpedia.[17]

The incapacitation or destruction of the states' IT assets, systems, and networks would have a debilitating effect on the security, public health and safety of our citizens, businesses, local governments, and academia. These sectors are increasingly dependent on state systems and services. The complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult. Declaring cybersecurity as critical infrastructure will provide the structure for coordinating public and private sector preparedness and protection.

This declaration of protection will allow for alternative funding capabilities, protection of operations and expeditious responses to emergencies. This protection would enhance the cybersecurity of state infrastructure; facilitate public and private consultation; establish frameworks for implementing cybersecurity minimum standards; and, maintain a cyber environment that encourages efficiency, cost effectiveness, innovation, and economic prosperity while also promoting safety, security, civil liberties, and privacy rights. It follows the guidance at the federal level and serves to complement currently available security measures.

In a 2020 report,[18] NASCIO, which represents state chief information officers, stated nearly half of all U.S. states do not have a dedicated cybersecurity budget line item. Most state cybersecurity budgets are between 0 and 3% of their overall IT budget compared with an average of more than 10% in the private sector. Minnesota's CIO faces an increasingly complex cybersecurity threat environment, and dedicated cybersecurity funding as a subset of overall IT budget would help give the Legislature and executive branch the right level of visibility into state cybersecurity expenses.

The Minnesota Legislature approved a $5 million increase for cybersecurity funding, which was a substantial accomplishment. As the complexities of cybersecurity attacks rise, so does the need to protect citizens' private data and a consistent source of funding will be necessary to best respond to and avoid events like the Department of Corrections ransomware attack.

17 Ballotpedia, Voter turnout in United States elections, https://ballotpedia.org/Voter_turnout_in_United_States_elections (accessed May 24, 2020)

18 NASCIO, Dedicated Cyber Funding Report, 2020, https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

Culture of Collaboration and Transparency

Through multiple demonstrations by agency representatives, executive branch personnel, and other partners, the BRC-IT learned that many of the challenges faced by the state are related more to individual behavior and perceptions than to actual technical or regulatory barriers.

This report contains specific recommendations regarding legislation, establishment of processes, assignment of responsibilities, and creation of roles, to address misperceptions. Transforming IT starts with first **knowing the required business outcomes** and then using technology to help deliver services to the residents of the state. It is not a one-time investment in a new application. Ongoing funds for maintenance, operations, upgrades, and replacement are key to long-term planning and funding.

Strong and effective IT leadership can advance this view. Likewise, state IT workers must be considered in future IT decisions. Minnesota is blessed with many hardworking, dedicated IT workers in the central IT function at MNIT and in the agencies. These professionals are key to the state's current and future success. Their careful hiring, ongoing development, and training and retention will help MNIT and the agencies fulfill their mission.

Strong and effective leadership will recognize the need to foster a **culture of collaboration and transparency** within MNIT but also with agency partners, counties, and other governmental units. For example, counties are often key members in the chain of implementation of state practices. A successful partnership between the state and the counties is required. Programs have flourished under such successful partnerships, while those with inadequate cooperation have faltered. This is frustrating to both parties, increases costs, and ultimately hurts citizens.

Through presentations and participation in the BRC-IT meetings, as well as multiple subcommittee meetings, county representatives of the Minnesota County Information Technology Leadership Association (MNCITLA) expressed to the BRC-IT a strong desire for more input into changes made at the state level and imposed on them for services that require their implementation and coordination. **Counties should not be an afterthought** for state agencies in relation to IT initiatives.

Finally, the early MNLARS experience of the BRC-IT stands as an example of the difference that transparency can make in an initiative. The Office of the Legislative Auditor's report on MNLARS indicated that key stakeholders in the project, the deputy registrars, did not have adequate representation in the process. This concern echoes those of the county representatives.

As noted above, the Chair of the BRC-IT prepared an independent expert review of the MNLARS project. It contained a recommendation to purchase a packaged software solution, a significant breakthrough and bipartisan solution after 10 years of difficulty. Complete transparency in this analysis and report ultimately led to the bipartisan solution.

In reading this report, it is important to consider the recommendations and principles not solely with an eye for their efficacy or effectiveness, but also with an understanding that they cannot stand alone. They will take place only within what Commissioner Tomes refers to as a "Connected Culture" – a culture of collaboration and transparency between the state and the people it serves.

Section 3

Section 3

Modernization Principles and a Modernization Review Board

> *According to a McKinsey Global survey of executives, the root causes of IT's ineffectiveness include "a lack of clear priorities for the IT function, weakness in IT's operating model, and talent issues." McKinsey Modernizing IT for Digital Reinvention*[19]

The essence of IT modernization is the identification and utilization of the best available technology to meet ever-expanding business needs. For private corporations and for public agencies alike, this can require substantial changes to the way in which IT organizations are structured and operate. The speed with which business/agency needs change requires agility that is simply not possible when tethered to old ways of working and when largely unsupported legacy systems form a significant portion of the IT portfolio.

A 2018 study by Accenture[20] concluded that (like state agencies) modernization requires federal agencies to 'break free of monolithic core systems that are especially common in government,' and that several factors contribute to higher technical debt, including:

- Irregular or prolonged funding cycles.
- Reliance on homegrown legacy systems.
- Persistent skill gaps.
- Leadership turnover.
- Risk-averse cultures.

The BRC-IT discussed all these topics as challenges that exist in Minnesota and need to be addressed. Moreover, the council emphasizes that effective modernization requires engineering the procurement or building the technology itself while *at the same time* ensuring **proper change management** – with sufficient stakeholder engagement in the need analysis, solution evaluation, planning, and adoption of the technology. Completing one of those things without the other ultimately leads to disappointment and failure. It requires close collaboration between IT services and the agency partner at every stage of a project or change initiative. There are so many moving parts and

19 Digital/McKinsey, "McKinsey Modernizing IT for Digital Reinvention," https://www.mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Modernizing IT for digital reinvention/Modernizing-IT-for-Digital-reinvention-Collection-July-2018.ashx (accessed May 24, 2020).

20 Accenture, "Decouple to Innovate: How federal agencies can unlock IT value & agility by remediating technical debt," https://www.accenture.com/_acnmedia/pdf-85/accenture-afs-decoupling-innovate-res.pdf (accessed May 24, 2020).

parties involved, however, so it is helpful to have some guiding principles to keep everyone pointed in the same direction.

Modernization Principles

A **clear articulation of modernization principles** helps to center all involved parties around important themes if they are frequently referenced and discussed. The BRC-IT discussed several examples of good modernization principles and some are reflected below. To ensure ready adoption and usage of the principles, agencies and MNIT would benefit from the exercise of identifying the principles they deem most important. As such, the BRC-IT recommends that agency and MNIT leaders take the next step of determining which require greatest ongoing focus for the State of Minnesota, and where further investment and focus are needed.

2. **MNIT should involve agency and technology leaders in the creation of business and technology modernization principles and establish a review process to ensure that the principles evolve as needed.**

Modernization principles can span many topics but at their center they are designed to guide the broader organization toward a **more strategic approach to deploying technology solutions** that ultimately help to improve usability, facilitate interoperability, simplify execution, and lessen the cost burden over the life of the technology. Leveraging industry standard software solutions for known business problems, adopting a set of shared technology platforms and patterns, and establishing a common approach for user experience are all examples of potential principles that can help a large organization ensure cost-effective, highly interoperable technology solutions. The BRC-IT recommends the themes on the following pages for consideration and encourages the working group of agency leaders and MNIT leaders to determine which make the most sense for the State of Minnesota.

Ensure a Beneficial User Experience

The BRC-IT explored possible benefits from leveraging human-centered design, agile principles and fostering innovation to challenge the status quo and ensure that true (versus perceived) business needs are identified and met. This requires MNIT and agency partners building practices that ensure strong, shared understanding of the needs of all customers and stakeholders today and into the future.

Cultivate a Learning Environment

Maintaining a team across MNIT and its partner agencies with sharp, current skills and perspectives is also critical to modernization. This requires continuous learning and development, both formal and informal, to keep pace with operational, technological, and cybersecurity changes, within a strong learning environment.

Communicate Clearly, Broadly, and Frequently

The BRC-IT also discussed the importance of developing a common language and ongoing dialogue around modernization, innovation, and the delivery of services among MNIT and its agency partners, as they strive together to deliver simple, effective solutions for all Minnesotans as they interact with their state's services. Agencies and MNIT must work collaboratively to achieve the modernization results Minnesotans deserve. This requires strong and frequent communication and regular stakeholder engagement, including tribal governments, counties, and other governmental units.

Create a Common Architecture

The BRC-IT discussed benefits of driving toward a common architecture including the reduction of risk, complexity and ultimately cost, better understanding of relations and dependencies, simplification of what-if scenarios, capability improvement, and greater confidence in future innovation.

Follow Security Standards and the Law

Multiple BRC-IT sessions focused on the need to keep up with industry standards for cybersecurity, and to monitor risk and compliance. The sessions illustrated how creating and maintaining a common architecture makes compliance with the law and with industry standards easier.

Promote Interoperability and Reuse

Further, sharing and reuse of IT solutions generally promotes greater interoperability, standardization, and cooperation among functions. To the greatest extent possible, data should also be shared among agencies rather than collecting the same data repeatedly and storing it in multiple places.

Over time, best practices find that the sharing and reuse of IT solutions results in more simplified, faster, and more efficient administrative procedures while reducing cost and saving time and effort. This is true of data, applications and infrastructure, and the BRC-IT recommends that MNIT and its partner agencies focus on such interoperability and reuse opportunities.

Maximize Benefit for the Enterprise as a Whole

In several conversations, it was apparent that agencies have varying technology needs. Some technology capabilities are required across all agencies; many more are shared needs for numerous, but not all agencies; and then there are some niche capabilities that might be critical for one agency but unnecessary for another. If MNIT and its partner agencies explore and delineate common and niche capabilities, they can maximize the impact of their efforts for the enterprise as a whole. While there may be a trade-off of cost and timing, best practices generally find that decisions that at least consider an enterprise-wide perspective and adopt shared platforms and shared patterns have greater long-term value than decisions made from any single organizational or agency perspective.

Leverage Industry Solutions

Sometimes, a custom build is unavoidable, but those situations are becoming more rare every year. Leveraging industry solutions may allow MNIT and the agencies to garner the benefits of the collective intelligence of the industry. It also usually avoids the looming dependence on unsupported legacy custom-built proprietary systems. Reusing readily available enterprise-wide solutions often offers a faster path to results, less risk and greater long-term value though it does not eliminate the software lifecycle that requires regular reconsideration of new vendors and the transition from one solution to another. MNIT and its agency partners should explicitly consider how a focus on industry solutions might further enhance their path to modernization and on whether installed or ‘as a service’ models make more sense for long-term maintenance.

Modernization Review Board

Establishing modernization principles is an important first step, but the principles will only deliver value when they are promoted, understood, and adopted across the enterprise – and they must be kept alive through regular review and appropriate edits. This can be done through the establishment and use of a Modernization Review Board.

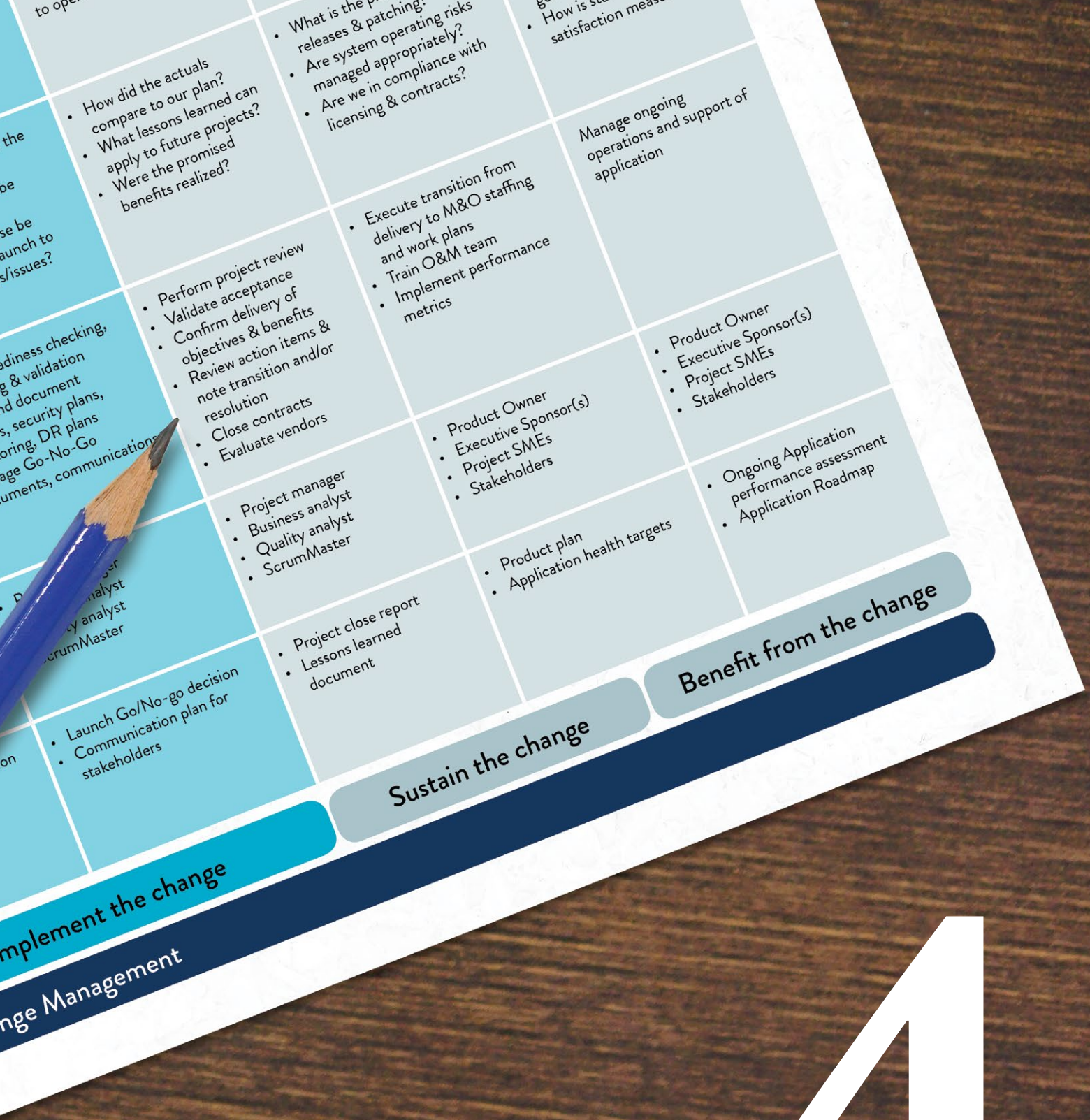
3. **MNIT should establish and host a Modernization Review Board (MRB) that includes key agency leaders to review the adoption of modernization review practices for large-scale or critical technology initiatives across the state.**

The goals of the MRB include:

- Mitigating risks and impacts to the business through technical due diligence and more informed decision-making processes for critical technology solutions.
- Optimizing and controlling costs through informed decision making, technology reuse and consolidation.
- Assessing adherence to the established modernization principles to reduce complexity, duplication, and cost in the enterprise.
- Assessing technologies for retirement and replacement.

Members of the Modernization Review Board will include the MNIT Commissioner and select agency and state partners to MNIT. This group will be supported by key enterprise and solution architects within MNIT. The ultimate goal is compliance with the modernization principles, but the BRC-IT understands that full compliance is simply not possible in all cases. With appropriate representation from MNIT and from the agencies, the MRB can minimize deviation but also ensure that agency needs are being met.

The Modernization Review Board could be modeled after MNIT's governing teams that include broad-based representation, like the Financial Steering Team, which is made up of agency CFOs who advise MNIT on enterprise rate and billing issues for IT services, and the MNIT Executive Steering Team, which is the key decision-making governance body within MNIT that provides oversight and steering to governance teams, provides direction for enterprise IT operations, and advises on IT utilization for businesses and agencies. The domain expertise from agencies brings valuable perspective to MNIT leadership and simultaneously maintains cross-enterprise coordination and understanding.


How did the actuals compare to our plan?
What lessons learned can apply to future projects?
Were the promised benefits realized?
What is the p... releases & patching?
Are system operating risks managed appropriately?
Are we in compliance with licensing & contracts?
How is st... satisfaction meas...
Perform project review
Validate acceptance
Confirm delivery of objectives & benefits
Review action items & note transition and/or resolution
Close contracts
Evaluate vendors
Execute transition from delivery to M&O staffing and work plans
Train O&M team
Implement performance metrics
Manage ongoing operations and support of application
Project manager
Business analyst
Quality analyst
ScrumMaster
Product Owner
Executive Sponsor(s)
Project SMEs
Stakeholders
Launch Go/No-go decision
Communication plan for stakeholders
Project close report
Lessons learned document
Product plan
Application health targets
Ongoing Application performance assessment
Application Roadmap
Sustain the change
Benefit from the change
nge Management

Section 4

Section 4

Modernization Playbook

Modernizing IT means ensuring that technology meets the current and emerging needs of the business. As business goals and needs change, the technology must flexibly adapt at the same rate.

> *According to Deloitte[21], 73% of state and local government officials believe their organizations are behind the private sector in terms of offering digital services.*

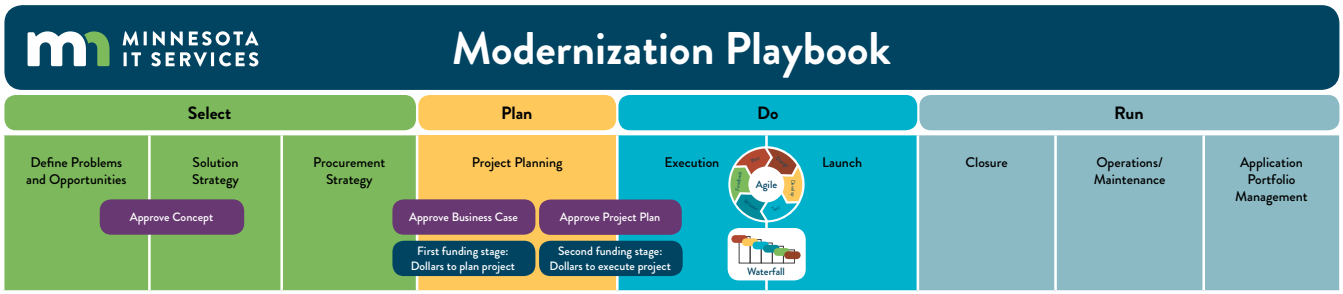
Modernization principles, such as those outlined above, set the general direction and approach to enable modernization. Beyond the principles, effective modernization requires that MNIT and its agency partners **leverage repeatable processes that reflect the modernization principles** and are well-understood by all participants across agencies and MNIT. To facilitate this need, the BRC-IT worked with MNIT to begin building a Playbook with more detailed guidance that can provide clarity about who needs to be involved, what questions need to be considered and what activities and deliverables are required.

> "As to methods, there may be a million and then some, but principles are few. The man who grasps principles can successfully select his own methods."
>
> —Harrington Emerson

Playbook Design & Development

In response to a BRC-IT recommendation in the December 2019 report, MNIT established a working group to create a Modernization Playbook with a high-level end-to-end view of the 'plays' required for successful modernization projects. Until the entire enterprise is walking in lockstep to the principles established, the Playbook serves as a useful guide to keep everyone moving in the same direction. It is not intended as an enforcement mechanism, but as a helpful quick reference guide.

21 Deloitte, "The Deloitte Digital Government Survey," https://www2.deloitte.com/us/en/insights/industry/public-sector/state-government-digital-transformation.html (accessed May 24, 2020).



Modernization Playbook stages

The Playbook is broken into four stages: Select, Plan, Do, and Run. It covers the processes and responsibilities associated with business case development, process analysis, stakeholder engagement, acquisition, solutioning with vendors, talent strategy, managing change, systems operations, system maintenance, cybersecurity, data management, portfolio and project reporting, and change management. The full text of the Playbook is available in Appendix I.

It aims to ensure appropriate business process reengineering with strong stakeholder engagement on every project by:

- Identifying the goals and objectives for each stage of the project.
- Calling out key questions to consider.
- Noting the activities and deliverables.
- Highlighting the relevant roles.

The working group creating the Playbook recognized the importance of effective change management throughout a project and calls that out at the bottom of the chart.

Modernization Playbook change management stages

Iterative design and development of the Playbook continues, and the working group is currently expanding visibility of the document, to gather additional feedback for improvement. Additional detail will be developed as challenges arise on IT projects. With proper reflection and root cause analysis, MNIT and agencies can iterate to improve the Playbook and suggest tools, information, and guidance for (and about) the activities and roles identified.

The BRC-IT views the following sections as critical attributes of the Playbook.

Business Process Review

First, MNIT and agencies must **seek to understand the business process** necessitating the technology before undertaking any significant IT modernization. Too often projects fail because new technology is forced into an existing business process that was built on old technology or built without human-centered design that focuses on the citizen or customer first. For example, the second key finding in the Independent Expert Review of MNLARS report was related to the fact that more work needed to be done to evaluate and simplify business process, rules, and regulations for a wholesale system replacement to be successful.

> "Several of the issues reported by stakeholders stem not from MNLARS itself, but from either antiquated or ill-defined business rules and processes or from incorrect data in the legacy system."
>
> —Independent Expert Review of MNLARS

It is time-consuming and difficult to truly understand not just how an old system works but why the old system was needed, what business need was being met – and then evaluate whether that same need remains or has changed. It is necessary, nonetheless, to map the existing processes and decisions, model the future process, and identify existing laws that create obstacles or legal changes that are needed.

4. **Agencies should evaluate and simplify business processes and rules before building, replacing or procuring new systems and make recommendations to the Legislature regarding modifications to laws and regulations.**

Plays related to business process review should emphasize that the responsibility is on the agency to articulate the business need and provide the business process expertise for this activity. In addition, MNIT and the agency must clarify the roles and responsibilities of MNIT and agency staff to perform this play well. MNIT has a responsibility to keep agencies informed about changing technology options and share best practices. With rapidly changing technology, agencies must keep an open mind about new technology options and opportunities, even if that means reconsidering the current business process. This business process reengineering may require resources the agency simply doesn't have, in which case it may be appropriate to consider using contractors to complete the review.

Vendor Engagement and Procurement

Vendor engagement is another activity in the Playbook that can greatly influence the results of a modernization initiative. In order to improve outcomes, strengthen security, and identify risks for the state, agencies must be able to engage early and often with vendors. After an informative presentation about procurement and several follow-up conversations with the Department of Admin and the procurement lead for MNIT, the BRC-IT concluded that Minnesota has procurement laws that do allow for the flexibility that is critical for modernization. In fact, Minnesota is viewed by other states as a leader in procurement policy.

> "Minnesota was one of the first states where the Legislature codified a 'Best Value' approach to awarding contracts, where the state considers a multitude of factors in addition to price. This, in addition to a flexible statutory framework, has allowed Minnesota to be a leader in inserting innovative approaches and techniques into our contracting processes."
>
> —Betsy Hayes,
> Minnesota's Chief Procurement Officer

Current law already allows for the agility agencies need to gather detailed information that enables better, faster decision-making about available solutions. Some agencies are exercising their ability to engage vendors more freely and earlier in the modernization process, and they are seeing good results.

As an example, the Department of Administration recently partnered with the Department of Transportation in issuing a **"Challenge-based RFP"** for connected and automated vehicle technology. This differed from a standard solicitation in that it focused more on stating the problem and requesting innovative solutions rather than the more traditional approach where the state is prescriptive in its requirements. The challenge-based approach has allowed the Department of Transportation to be early adopters of innovative technology, engage with vendors in a positive and open way, and ultimately emerge as a leader in the area of connected and automated vehicles.

Still, this flexibility might not be apparent to all agencies. Amending statutory law slightly or providing a clear interpretation of current statutes will enable innovative and faster procurement. Even a simple education campaign would be beneficial.

5. **MNIT and the Department of Administration should develop and implement a plan to ensure that agencies understand and use their authority and ability to engage more fully with vendors before a final vendor is selected.**

It would be even more beneficial to provide a central knowledge resource to support procurement activities for large-scale IT modernizations.

6. **MNIT should build capacity within the procurement unit to develop procurement strategies and support acquisitions for IT modernization projects.**

Vendor Risk Management

When a third-party vendor is engaged, it is imperative to ensure that due attention is paid to securing the state's data and systems from potential security threats. The vendor must provide evidence that their security controls are aligned to security best practices. The increasing frequency, creativity, and variety of cybersecurity attacks means that all agencies interacting with vendors need to ensure cybersecurity risk assessments are completed to have an effective risk management program.

The State of Minnesota currently uses a structured vendor risk analysis process to assess the risks associated with the vendor and its products and services. A review of this current process is needed to ensure alignment with the chosen MNIT security framework architecture and that a comprehensive approach is applied to identify, mitigate, and track risks. This helps align to IT security best practices and includes adequacy of vendor information security controls, physical security considerations, and business continuity plans to minimize risks to the state's data assets. Providing a process that integrates security and risk management activities into the vendor lifecycle is imperative and required for **securing information and systems**.

7. **MNIT and the Department of Administration should jointly assess the current vendor risk through a structured process and security framework for contract management and risk prioritization.**

8. **MNIT should provide education for agencies on the IT security risk assessment process and partner with agencies to assess, manage, prioritize, and communicate any risks encountered during the process.**

Privacy Impact Assessments

Organizations have adopted the use of a privacy impact assessment (PIA) as part of their process of determining the potential data privacy implications of projects. First adopted broadly by the federal government as part of the E-Government Act of 2002, privacy impact assessments demonstrate how federal agencies handle or will handle American citizens' private data collected in the operation or development of systems. The act requires that federal agencies conduct a privacy impact assessment before developing or procuring IT systems or projects.

Privacy impact assessments have been adopted in the private sector, as well. Delta Airlines, through its chief privacy officer, conducts privacy impact assessments for any new technology or process implementation. According to Renee Lope-Collnetta, the CPO for Delta, no project can close without submitting a privacy impact assessment and getting a response from the Chief Privacy Officer.

Conducting privacy impact assessments at the beginning of IT projects will ensure that all stakeholders in the project satisfactorily answer a set of privacy impact questions. Conducted in accordance with the framework established by a CPO[22], in consultation with key data management stakeholders at MNIT, the privacy impact assessment can **prevent damaging and potentially costly complications of data privacy problems** resulting from a new project.

9. **Agencies should conduct a privacy impact assessment for all information technology projects as part of the project initiation process.**

The privacy impact assessment should function as a tool to ensure project sponsors and agency leaders understand the data and privacy implications of new technology, programs, or ways of doing business. The privacy impact assessment will also lead to more uniform adherence to enterprise privacy policies as well as enterprise data management and data sharing standards.

22 More information about the Chief Privacy Officer recommendation is in Section 5: People Enabling the Modernization Vision.

Portfolio Reporting

With the broad range of enterprise and agency-specific responsibilities, MNIT has a large portfolio of systems and projects to monitor. Some of the project and program performance data is useful for all to see. Some of it is useful for a select audience. Without proper analysis and thoughtful organization though, it is useful to nobody. Modernization requires that we understand where we are now and where we are going in order to measure our progress toward that goal. A portfolio report or dashboard is an effective way to share that progress.

MNIT knows that IT is just one of many things that agency leaders must divide their attention between to effectively execute on their missions. Making IT reports easy to consume and actionable **helps leaders make quick, informed decisions**.

MNIT's Enterprise Portfolio Management Office (ePMO) is designed to support MNIT leadership and other key stakeholders as a trusted source of data on the state's project portfolio and enable high-level decision-making on the over 350 projects in progress at any one time. The ePMO provides guidance and oversight for MNIT's large and broadly distributed portfolio of IT projects to help mitigate risk. The work of the ePMO is informed by and complies with statutory requirements.

Agency leaders need to see a near real-time report of current projects with forecasted and actual costs. MNIT is developing a financial reporting model to provide information about actual project costs. Agency leaders and legislators should also see project outcome reports detailing how projects align with the state's priorities.

MNIT has made progress increasing the transparency of its project portfolio reports through several initiatives including improved reports to the Legislature; implementation of online project management software; outreach to agency-based PMOs; and formalization of project reviews with MNIT's Executive Steering Team. While these improvements demonstrate significant time and resource investment in the continued maturity of the ePMO, gaps still exist in the effort to provide a holistic, real-time, publicly available dashboard to support stakeholder engagement and decisions.

To address the gaps, the following is required:

- Agreement between the MNIT Commissioner's Office, the agency commissioner's office, and the MNIT PMOs at the agency on the criteria for which projects to report in the dashboard.
- Consistent and commonly applied processes for reporting on project process.
- Decision as to what information would be of most value to report beyond the standard scope, schedule, and budget metrics.

10. MNIT should establish a plan for real-time access to project and portfolio management reporting that ensures effective communication with all stakeholders.

Spend is just one of many components that MNIT and agencies must monitor. To break away from the heavy dependence on legacy systems, we must know which legacy systems exist, what support is provided to keep them running, and how much money is spent. Examples of other components include business value and technical condition that can help identify legacy systems in need of replacement or elimination. Agency leaders rely upon MNIT to supply up-to-date information about the agency's existing applications and about ongoing technology projects. With accurate and timely information that comes with data transparency, agency leaders can make fact-based decisions. More information about the current state of MNIT dashboards and plans for the future is available in Appendix J.

Playbook Implementation and Adoption

The BRC-IT is pleased with the first draft of the Playbook, a collaborative effort between private and public sectors and business and IT leaders, and believes it will be a valuable tool for staff at MNIT and agencies alike. The one-page summary of the Playbook is simple enough to provide a general understanding of the whole process of modernization while complex enough to address the many different facets of effective and efficient execution.

As with the modernization principles, the Playbook will only be effective with widespread knowledge of the purpose behind it, the plays included in it, and the associated roles and responsibilities of the many people involved in modernization projects. Acceptance by state leaders is required to maximize its effectiveness. Although the Playbook is designed as a guide for state leaders, MNIT must play the lead role in raising awareness about IT modernization and the Playbook to ensure full implementation.

11. MNIT, working with state agency partners, should create education and training to introduce the Modernization Playbook to all MNIT staff and agency leaders and draft a plan to drive, govern, and measure adoption and acceptance of the Playbook.

As in any corporation, some of the concepts in the Playbook are already embedded and fully embraced by certain teams at MNIT. The same concepts might be unfamiliar to others. MNIT should strive for continuous improvement for all teams regardless of their current practices, encouraging regular reflection on what is working and not by soliciting feedback from both agency and MNIT staff. It might also be helpful to look at other playbooks in use, like the Digital Services Playbook[23], created with input from private and public sector experts and published by the U.S. Digital Service.

If implemented effectively, agency leaders will be better informed about the strengths and weaknesses in their IT portfolio, MNIT will make steady progress toward modernization, and citizens will experience the benefits of more agile and innovative IT services.

23 Chief Information Officers Council (CIO) Council, "U.S. Digital Services Playbook," https://playbook.cio.gov/ (accessed May 24, 2020).

Section 5

Section 5

People Enabling a Modernization Vision

Strong and thoughtful leadership is required to create an innovative culture of statewide partnerships to meet the increasing digital demands and a growing ecosystem of connected devices, websites, and secure online services in state government. As the leading technical agency for enterprise information technology development, MNIT needs to establish clear roles and responsibilities for its staff, the agencies, and other partners to enable the vision of modernization and secure data and systems for all.

The depth and breadth of work to be done is staggering when considering the fact that MNIT works with more than 70 agencies, with local and tribal governments, with education, and some non-profit organizations. Their teams develop, maintain, and secure the state's IT infrastructure and private data. An **effective technology governance strategy with clear roles and responsibilities** is imperative to build modern systems and secure applications.

Agency priorities differ, as do their needs, and agency leaders need clear guidance that will help them to evaluate risk and make decisions related to the technology required for their respective mandates. Currently the division of responsibilities between MNIT and state agencies is unclear for various IT services. Agency staff and leadership are not always familiar with their obligations OR with the services available to them, and clear roles and responsibilities supported by frequent communication efforts will help to create the connected culture.

Agencies, in partnership with MNIT, must take responsibility for monitoring trends and best practices as the demand for digital government services continues to grow. Innovation around the user experience, advancing cloud-based technologies, securing private data, and adapting procedures to rapidly changing circumstances while remaining true to the policy goals established in legislation are priorities.

High-quality information technology starts with the leaders.

Leadership

The Chief Information Officer (CIO), Chief Business Technology Officer (CBTO), and Chief Information Security Officer (CISO) roles are clearly established at MNIT. The creation of a chief privacy officer (CPO) role is recommended and described below. This new role would be housed outside of MNIT and have the responsibility to coordinate and support the development and application of a consistent approach to data privacy across state agencies.

Chief Information Officer

The state CIO sets IT strategy, direction, policies and standards for enterprise leadership and planning for MNIT. This role provides oversight and direction for IT policy and management, delivery of services, and security of private data. The CIO manages the strategic investments in IT systems to ensure secure access and efficient delivery of accessible government services to maximize benefits in its enterprise role. He is supported by three enterprise service leaders who further enable the essential operations of agency-specific services.

Chief Business Technology Officers

Chief Business Technology Officers (CBTOs) serve as the primary liaisons between MNIT and the agencies. They work closely with agency leadership to manage IT services and budgets at the agency level. CBTOs help set the "future direction, goals, and priorities" for IT at agencies. They have considerable latitude to make decisions about how to deliver agencies' IT services within the confines of the agencies' available resources.

For historical reasons and variations in agency needs, about half of the CBTOs work exclusively with one agency, while the others serve two or more agencies.

Current breakdown of CBTO assignments

The 2019 Evaluation Report of the Office of Minnesota Information Technology Services by the Office of the Legislative Auditor indicated a perceived gap in MNIT's understanding of the agencies' business needs. Technology is a critical component of the successful delivery of agency services. The CBTO is the IT leader for the agency. Accordingly, the BRC-IT finds that MNIT should reinforce the CBTOs access to agencies' executive-level meetings and decisions.

12. **State agencies should include the CBTOs in the agencies' various leadership teams and include them in the highest appropriate level of leadership meetings and strategy planning.**

Chief Information Security Officer

The CISO establishes, oversees, and facilitates statewide security management programs to ensure government and citizen information is protected. Responsibilities include:

- Creating statewide security policies and IT standards.
- Requiring information security plans and annual assessments.
- Requiring security awareness training for employees.
- Identifying, reporting on, and controlling incidents.
- Monitoring threats and taking preventive measures.

Chief Privacy Officer

Like the value inherent in a dedicated leader focused on security, the BRC-IT believes there is value in having a dedicated leader for data management and governance. Members of the private sector and agency representatives who have examined data governance practices across the country have indicated that a dedicated privacy officer is increasingly valuable to private- and public-sector organizations. In addition, an organization like the State of Minnesota has many agencies with individual data governance policies in place, and a chief privacy officer can serve as a go-to resource for policy development and training to standardize data privacy policies and guidelines across executive branch agencies.

13. **The executive branch should establish a chief privacy officer position to support state decisions about data privacy and sharing.**

While some agencies have their own mature data privacy practices in place and should continue to leverage their experience and subject-matter expertise related to data privacy and management, a chief privacy officer can bring great value to the state. In this role **the CPO will**:

- Act as a key subject matter expert and resource for agencies regarding policy and practice.
- Fill the gap for smaller agencies, boards, and commissions that don't have their own data privacy expert.
- Convene and coordinate with agency privacy officers to help establish consistency with respect to policies being applied across the executive branch.
- Develop a privacy impact assessment and support the consistent use and application of these assessments across the executive branch, by MNIT at the start of large IT Initiatives.

The BRC-IT conversations about the establishment of this CPO position revealed a variety of views about the role and associated responsibilities, with some preferring a stronger centralized authority on policies related to data privacy practices, and others preferring that the CPO focus on providing support and advice to agencies, which have ultimate responsibility for their data consistent with their statutory authority and the federal programs which they manage. The BRC-IT recognizes the CPO can be successful and add

value in a variety of configurations. The BRC-IT also expects a new office will likely start as a smaller advisory role and evolve over time into an office with greater authority, if deemed appropriate by policy makers. Additional potential roles and responsibilities of the CPO that were discussed are listed in Appendix L.

The state's Chief Privacy Officer should be **housed outside of MNIT** to be most effective. The privacy officer should work closely with individual agency and MNIT staff charged with information security, cybersecurity, and data management to ensure consistent application of enterprise policies across common areas of responsibility.

The Chief Privacy Officer should also be **separate from the state's Data Practices Office**. The Chief Privacy Officer's focus should be guiding and coordinating executive branch's data privacy efforts, while the Data Practices Office's mission is to provide assistance and advice on data practices and open meetings to the public and government. The DPO's focus is on compliance with the MDGPA, and it exists to serve a much larger community of interest than the state's executive branch. Additional detail about the MGDPA is available in the box below.

Appendix K includes a list of states with a chief privacy officer.

The Minnesota Government Data Practices Act

The Minnesota Government Data Practices Act (MGDPA)[24] dictates how governmental data is treated and used in Minnesota. It dictates what information can be collected, who may see or have the information, classification of specific types of government data, and procedures for applying classifications, the duties of government personnel in administering the provisions of the MGDPA, procedures for access to the information, civil penalties for violations of the MGDPA, and fees for copies of the data.

Housed at the Minnesota Department of Administration, the Minnesota Data Practices Office (DPO) is charged with providing advice and assistance to the public and governmental entities on application of the MGDPA. The DPO also assures that the state's open meeting law is properly applied and followed, and it can offer non-binding advisory opinions on data-related questions within state government.

While the objectives of the DPO and the mandates of the MGDPA intersect with the data privacy and management considerations of the BRC-IT, our interest lies in supporting strategies to gather and use data to maximize stakeholder value in the manner cited by the Pew Charitable Trusts' study (see Footnote 29). The BRC-IT identified opportunities for advancement of data management for the benefit of state agencies, partner organizations and governments, and other stakeholders.

24 State of Minnesota, Department of Health, The Minnesota Government Data Practices Act, St. Paul, Minn., https://www.health.state.mn.us/communities/practice/resources/chsadmin/data-mgdpa.html, (accessed May 24, 2020).

Hiring, Developing and Retaining Talent

Keeping pace with technology change is especially challenging to the state workforce. It requires agencies and MNIT to recruit and retain business analysts and data analysts to understand the agency business processes and outcomes. It also requires MNIT to recruit and retain a workforce that is resilient to change and can continuously learn and adapt to a changing technology landscape including cybersecurity threats. MNIT will also need an onboarding and ongoing workforce development program to provide a foundation in business principles and effectively apply the guidance in the modernization playbook.

Facilitating an innovation mindset and a culture of inclusivity and improving cross-agency talent development is critical to following a human-centered design approach and walking in the shoes of those who rely on the systems they build and maintain. Providing a space or structure for employees to innovate with customers will give employees the options to grow and develop their skills.

Cybersecurity Training

Minnesota's stakeholders include individual residents, citizens, and visitors – also communities, businesses, and local and tribal governments. They have high expectations that the state will maintain trust in systems when it comes to data and privacy protection. They trust that technology, processes, and people are aligned and trained to manage and secure their very sensitive personal data.

People are generally unaware of most cybersecurity risks. As new devices are connected each day, more sensitive data is transferred which increases vulnerabilities. The top three threats identified in the 2019 Deloitte-NASCIO Cybersecurity study are: phishing, social engineering, and ransomware. In its 2019 Annual Report, MNIT stated that employees are often the weakest link in an organization's security defenses. Since 1993, MNIT has managed Minnesota's Network for Enterprise Telecommunications (MNET), the state's dedicated public sector network. MNET connects all 87 counties, 300 cities, and 200 public higher education campuses across the state, including legislative and judicial branches. This makes for a very wide network of people.

Likely in response to those threats and the fact that *people* are often the point of vulnerability, most states—94% in 2018, up from 84% in 2016—deliver cybersecurity training to state employees and contractors at least annually. Some states include third-party vendors and legislative, executive, and judicial branches. A document prepared by the NCSL indicates states vary in making cyber training voluntary or mandatory.

MNIT is responsible for training the executive branch on cybersecurity practices. Limiting this offering to executive branch staff prevents the state from **realizing the full benefit of an enhanced information security posture**.

Though not required, offering MNIT's cybersecurity training to legislative and judicial branch employees would help secure sensitive data that MNIT is required to protect. IT literacy and cybersecurity training are vital for all state employees. All need strategy-related communication, and they need end-user training. Sharing of best practices needs to be commonplace for all. Due to rapidly changing technology, training should be deeper than standard end-user safeguards, and should achieve the goal of enabling informed decision-making on matters of modernization, cybersecurity risk assessment, and data management.

Because of the important role they play in guiding priorities and approving funding for IT modernization and cybersecurity, it is strongly recommended that legislators participate in cybersecurity training. Cybersecurity training for the legislators must follow consultation with

legislative leadership, in recognition of the fact that imposing such a requirement on elected leaders is complicated. Still, this training for legislative leaders is strongly recommended for the assurance to understand what is required to protect the citizens of Minnesota.

14. **MNIT should establish an awareness campaign and a cybersecurity education and training program that can be made available to legislators and others in state government.**

Partnership and Collaboration

To build upon the Connected Culture ideology called out in its Tactical Plan,[25] MNIT must continue to tap external talent to advise and support the CIO and CISO. Minnesota has a strong culture of volunteerism and is noted for its exceptional talent. Establishing formal advisory bodies and informal networks to gain expertise from the private sector, from legislators, and from municipal groups would greatly benefit the state, especially for large IT projects.

BRC-IT conversations generated support for advisory roles that would bring additional expertise and perspective to state government. For example, a Skilled Professional Program would bring valuable insight; a Cyber Civilian Corps could serve as a forensics group for smaller governmental partners throughout the state; and a Legislative Cybersecurity Commission would be beneficial as a secure group that would receive frequent updates on cybersecurity issues.

The BRC-IT feels that engaging other governmental units such as the Minnesota County Information Technology Leadership Association (MNCITLA) and tribal governments early in the development process will improve efficiency. It is important to recognize their talent and their role in successful implementation of large projects.

Skilled Professional Program

A Skilled Professional Program aims to match private-sector experience with a specific need in the government-sector or non-profit. There are many needs within IT services that are difficult to meet. This is true for a variety of reasons, including but not limited to salary caps and labor shortages. MNIT would benefit by bringing executives and domain experts into conversations about cybersecurity, data management and privacy, modernization of the IT infrastructure, and culture. Professionals could work for the state for a limited period in a structured program. For example, a corporation could lend the services of a senior architect for a one-year term.

An arrangement like this would be mutually beneficial, offering the professional some experience in a complex governmental organization with multiple (sometimes conflicting) parts while providing the state the benefit of private corporate sector talent and perspective in a project, especially in high-level roles that may otherwise be difficult to fill.

The BRC-IT now knows this arrangement is both possible and valuable. With no hesitation from either side, Ecolab recently loaned an executive to work on the Governor's COVID response team. On April 20, 2020, Governor Tim Walz and Ecolab CEO Doug Baker announced the assignment of Ecolab President of Global Regions, Jill Wyant, to the Critical Care Supply Working Group. The working group's goal is to ensure that critical care equipment, including personal protective equipment (PPE), will be available to ensure hospitals have the supplies they need when

25 The Tactical Plan is available in Appendix H, along with MNIT's Guiding Principles & Priorities.

faced with increasing infections of COVID-19. Wyant enlisted the assistance of Minnesota's top companies to share their talent with state purchasers. The expertise of private-sector supply chain management is instrumental in this arena where Minnesota is competing not only against other states, but also from other countries. The close coordination with corporate partners allowed the state to quickly vet potential vendors, determine at the point of production whether a product met the state's standards and needs, and manage international logistics. In the race to secure supplies, that assistance saved valuable time and resources critical to meet a desperate demand.

The Covid-19 event highlighted the need for private-sector collaboration. Several businesses stepped up to assist. BRC-IT believes MNIT could benefit from ongoing private sector expertise on organizational change management as well as IT policies, practices and procedures.

15. **MMB should assess the feasibility of a Skilled Professional Program, identifying the appropriate authority for the program and whether statutory changes are required, and then present their findings to the BRC-IT.**

Other skilled professional programs can serve as models. Some examples are available for review in Appendix M.

Cyber Civilian Corps

In late 2019 and early 2020, nearly 35 states, Washington D.C. and Puerto Rico enacted or introduced legislation to create cybersecurity task forces, commissions, councils or civilian corps to study and advise on cyber-related issues. More than 365 bills or resolutions were introduced and are highlighted by the National Council of State Legislators (NCSL). The areas seeing the most legislative activity include:

- Requiring or incentivizing government agencies to implement training and education or specific types of security policies and practices and improving incidence response and preparedness. Increasing penalties for computer crime or addressing specific crimes, e.g., ransomware.
- Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.

Michigan's MIC3 Program

The state of Michigan was the first in the country to create a cyber civilian corps, named MIC3 in 2013. Its focus is to offer forensics services to address critical IT and cyber issues. Its cyber forensics format is based on that used by the Department of Defense. MIC3 also created an internet of systems or "range" used for testing with hospitals, school systems, and industrial control systems.

Consisting of forensics professional volunteers, MIC3 responds to critical requests for assistance from local government, municipalities, and schools. Their expertise is spread geographically around the state to ensure instant forensics responses. There is a high bar to entry, the members must have the knowledge and forensics capability to respond to cyber-attacks and all members must pass a background check.

MIC3 has served the state well as it reaches out and offers much needed expertise to localities that may not have that talent on their staff.

Minnesota has a world class cyber range located at Metropolitan University in St. Paul. The MN Cyber Range[26] hosts a training and simulation platform that uses real-world scenarios and innovative technologies to ensure cyber defense teams have the knowledge and experience they need to protect crucial information, systems, and operations.

Creating a responsive public and private cybersecurity partnership to deploy volunteers upon the occurrence of a cybersecurity incident, will increase resiliency and protection for all across the state of Minnesota. This Corps would bring together best practices and capabilities to share technical knowledge to help support common cyber infrastructure strategy, alignment of security standards and commonality of practice for governmental units and tribal governments.

16. MNIT should explore the feasibility and, if appropriate, outline a plan for creation of a public/private partnership for cybersecurity.

Legislative Coordinating Committees

BRC-IT members believe there are additional opportunities for collaboration and communication, for both cybersecurity specifically and information technology more generally, within the Legislature. Legislative coordinating committees can be an effective way to raise awareness within the legislature and to ensure there is a bipartisan effort to explore and examine IT-related issues even outside of legislative sessions. They can review Minnesota's practices as compared to industry standards on things such as cybersecurity spending, and they can help provide guidance and understanding about system improvements and upgrades from being a 'one and done' expenditure to an asset that requires ongoing maintenance.

17. The Legislature should create two new legislative coordinating committees – one for cybersecurity and one for technology.

The Cybersecurity Legislative Coordinating Committee would be the key body to hear the status of the state's cybersecurity protection, support adequate funding for cybersecurity programs, and help educate and raise awareness of the criticality of the issues. The Technology Committee could discuss IT policies, spending, and reports and dashboards; educate members and their peers; and help secure necessary and appropriate IT funding by raising awareness about product lifecycles and the IT portfolio within a larger group of legislators.

With the increased digitization and connectedness of devices, operational technology, and IT systems that are used across critical infrastructure sectors, it is imperative to improve cybersecurity preparedness and response. Currently there isn't a mechanism to provide security information to the Legislature in the event of a major breach.

In addition, based on other significant recent events—such as those in Atlanta, Georgia; Baltimore, Maryland; Houston, Texas; Pensacola, Florida; and New Orleans, Louisiana—the BRC-IT is recommending the creation of a Cybersecurity Commission within the Cybersecurity LCC. This commission would give members the opportunity to receive briefings on sensitive cybersecurity information, to serve as a crisis management team and an ongoing operational committee for IT security. Procedures would be established for the legislators to have appropriate security clearance

26 Metropolitan State University, Minnesota State IT Center of Excellence, MN Cyber Range, https://mncyber.org/cyberrange/ (accessed May 24, 2020).

and the consideration to hold closed meetings for briefings on the current condition of cybersecurity for the State of Minnesota. With the ability to meet in private and with appropriate security clearance, this commission can review in-depth IT security and advise on building an executive dashboard on the health of cybersecurity at the state. A major breach would be devastating to Minnesota's safety and economy.

House File 4536[27] was introduced in April 2020 to create a Legislative Commission on Cybersecurity. A bill to create a Legislative Commission on IT has not been introduced.

Other Governmental Units

State agencies initiate projects and develop programs that rely on data shared with, used by, and needed by counties to deliver services to the people living in those counties. Those projects and programs can be more effective, with fewer implementation and budgetary concerns, if the counties are involved at the outset of project development and throughout the lifecycle of the program.

The Minnesota County Information Technology Leadership Association (MNCITLA) was created in 2004 and has grown to a membership of over 60 counties, actively sharing ideas, collaborating on projects, and equipping county technical staff with the collective knowledge of other counties, large and small. MNCITLA offers significant technology knowledge, experience, and boots-on-the-ground insight into data practices policies and how they affect their delivery of services. Over the years, members of MNCITLA have been involved as subject matter experts in various policy workgroups and committees at the regional and state level. MNCITLA has expressed interest in earlier and active participation in the development of programs that have an impact on their services, so their data needs and challenges are aligned with those of the sponsoring state agencies.

Representatives from other governmental units and tribal governments can also bring value to the state by participating in the early stages to consider interoperability between state and county systems in establishing data practices policies. Their participation will add practical insight to decision-making and foster faster acceptance. The state should take advantage of their experience. It also helps avoid complications that arise from implementation of large programs by establishing shared goals and responsibilities.

18. MNIT and state agencies should include other governmental units (including MNCITLA) and tribal governments as partners at project launch and include an assessment of their data needs and challenges in establishment of data privacy and management policy.

In some cases, state agencies have developed and implemented projects involving county systems with no county IT involvement on the front end. This has an impact on them in terms of logistics and budget. This is particularly acute in small counties with limited funding and resources in comparison to the larger counties to absorb new costs and mandates. Involving them from the beginning can help avoid gaps in delivery, data concerns or technical complexity and MNCITLA has noted the need for standardized solutions and less complexity for their counties.

27 The full text of HF4536 can be found in Appendix F and at https://www.revisor.mn.gov/bills/bill.php?b=House&f=HF4536&ssn=0&y=2019.

Section 6

Section 6

Enterprise Strategy for Modernization

Using the framework outlined above to 1) identify principles, 2) follow a Playbook, and 3) clarify roles and responsibilities, we are confident in MNIT's ability to modernize, but it will require strategic planning and deliberation - and close collaboration between agency and technology teams to socialize the framework and build an Outlook, a long-term strategy for both the agency to deliver on its mission and for MNIT to provide the appropriate technology that the agency needs. It requires an enterprise-wide governance strategy for modernization activities, including cybersecurity efforts, and for data management. There are still many details to discuss, with participation in those discussions required from agencies and MNIT as well as from legislators.

> *"End-to-end modernization, or a holistic approach to tackling system upgrades, completely redefines how a company thinks about IT. Under this approach, the technology organization is no longer just a shared service; IT becomes a critical part of the company's DNA, and IT leaders become trusted partners, not just service providers." McKinsey*[28]

Co-creation of a Modernization Outlook

With a significant variance in the size of agencies and a wide variety of responsibilities, there are substantial differences in IT capabilities and in the bandwidth to deal with IT issues from agency to agency. Likewise, agencies have different priorities when it comes to IT generally and IT modernization more specifically. MNIT must balance the need to serve the collective enterprise with the need to provide agency-specific services, and seek to

28 McKinsey, Modernizing IT for a Digital Era, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/modernizing-it-for-a-digital-era

understand the burden on the different agencies 1) to follow enterprise-wide principles; 2) use enterprise-endorsed tools and systems, and 3) engage effectively in modernization activities, even with a useful Playbook. Cybersecurity is an important example of a MNIT priority that may weigh more heavily on some agencies than on others. Only through frequent and active collaboration can MNIT understand this burden and the business needs each individual agency is tasked to meet.

19. **MNIT should collaborate with agencies on the development of a 10-year Outlook for business modernization and the related 5-year plan for technology modernization.**

Every agency has a vision for how best to serve the citizens of Minnesota. Many of their ideas require technology of some sort – if not for an external-facing application, then at least for internal purposes. A 10-year **Business Modernization Outlook** gives the technologists a big-picture view of these ideas for service. With this business outlook, MNIT can provide higher quality service to agencies and is in a better position to more effectively evaluate the technology options that may suit the need.

> "Only about one-half of state agencies said that MNIT understands their business needs."
>
> — Feb 2019 OLA Report

Reviewing and discussing the modernization principles and the Modernization Playbook should be part of this Outlook development. After review, each agency should be able to articulate what is possible under their current operating model and what must change to be able to abide by the principles and follow the Playbook and achieve the Outlook with proper consideration of cybersecurity. They might identify skills that just don't exist – or roles that need to be filled. Some business processes or project methodologies may need to be reconsidered – and together, MNIT and agencies need to evaluate how to change the current IT funding model to expedite modernization progress. With clarity around agency goals and priorities and an understanding of the current gaps, each agency can, in close collaboration with MNIT, establish a five-year **technology Modernization Outlook**.

Co-creation of a Data Management Strategy

Data grows increasingly important in the lives of Minnesotans. With thousands of applications in use, state and other levels of government collect massive amounts of data. Effective governing going forward requires using that data in a planful and effective manner. It may also require simplification of laws around data practices.

In a study[29] conducted by the Pew Charitable Trusts, 350 state officials identified several key areas in which data analytics helped in state government decision-making:

- Crafting policy responses to complex problems.
- Improving service delivery.
- Managing existing resources.
- Examining policy and program effectiveness.

29 Pew, "The 2018 Pew Charitable Trusts study, How States Use Data to Inform Decisions," February 21, 2018, https://www.pewtrusts.org/en/research-and-analysis/reports/2018/02/how-states-use-data-to-inform-decisions (accessed May 24, 2020).

The BRC-IT recommends that MNIT also begin to examine the possibility of enterprise data management.

20. MNIT should convene a working group of MNIT and agency staff to present a plan to catalog all data managed by the state, establish a metadata framework that enables data sharing and system interoperability, and identify guidelines for retaining and purging data.

Strategic data management can begin with agencies and MNIT identifying and purging data on an ongoing basis as aligned with best practices, particularly private and nonpublic data, that is no longer necessary for agency functions or required by law to be maintained. In addition, key responsibilities to be assigned to MNIT under this recommendation are those of facilitating the interoperability of data; supporting the development of a catalog of data sets and data sharing agreements; providing data warehouse support, guidance, and standards; and advocacy for the removal of unnecessary or high-risk data sets.

In the publication Data Governance Part III: Frameworks – Structure for Organizing Complexity[30], NASCIO cites examples of working data governance framework, including those of the Data Management Association (DAMA), the Data Governance Institute (DGI), and IBM. These models all include components similar to those identified as MNIT's key responsibilities in the area of enterprise data management governance and support.

Data management plays a critical role in effective IT operations, and a properly forward-thinking organization must have building blocks for strategic data management in place to leverage data effectively. This applies to private and non-governmental organizations, and governmental agencies alike. According to the National Association of State Information Officers, however, this strategic approach to data management in state government has some specific challenges. In particular, state government has a history of managing information in a decentralized manner.

Strategic data management should play a central role in IT development and modernization efforts in order to minimize these historical consequences. The following are examples of strategic data management practices and principles:

- Consider data collection prior to the initiation of IT and modernization efforts.
- Define data maintenance guidelines or requirements prior to the initiation of IT development or modernization efforts.
- Consider data usage prior to initiation of IT development or modernization efforts.
- Gather data intentionally, with a focus on the value that data can provide.

For example, an intentional approach might be to minimize the collection of unnecessary data on individuals (including personally identifiable information, also known as PII) to limit the risk of maintaining that data.

30 NASCIO, NASCIO Governance Series, "Frameworks—Structure for Organizing Complexity," May 2009, https://www.nascio.org/wp-content/uploads/2019/11/NASCIO-DataGovernancePTIII.pdf (accessed May 24, 2020).

Different agencies through the state have varying levels of maturity in their data governance and data sharing. While there have been improvements enterprise-wide in these areas, other states have taken more direct steps toward formalizing and prioritizing data sharing through executive order, legislation, and memoranda of understanding.[31]

> *Cumbersome and idiosyncratic data access procedures create confusion, impose unnecessary costs, and are a barrier to evidence building without always providing significant privacy benefits*
> *—The Promise of Evidence-Based Policymaking*[32]

Just as the state needs an entity responsible for developing and administering privacy policies (a chief privacy officer), it needs a single source for guidance and support for enterprise data management and governance. Bringing this responsibility into one agency can help reduce some of the inefficiencies and inconsistencies between agencies that currently exist. It can also help reduce and refine the data sets the state houses overall.

MNIT should be recognized as the lead agency for enterprise data management governance and support. This means MNIT will provide as much support to agency partners as necessary to ensure a consistent and business appropriate management of enterprise data. Successful implementation of enterprise data management practices requires a play in the Playbook related to evaluation of the data collection, maintenance and usage that is associated with the legacy system and the new solution, with special attention paid to personally identifiable information (PII) and privacy concerns that may exist.

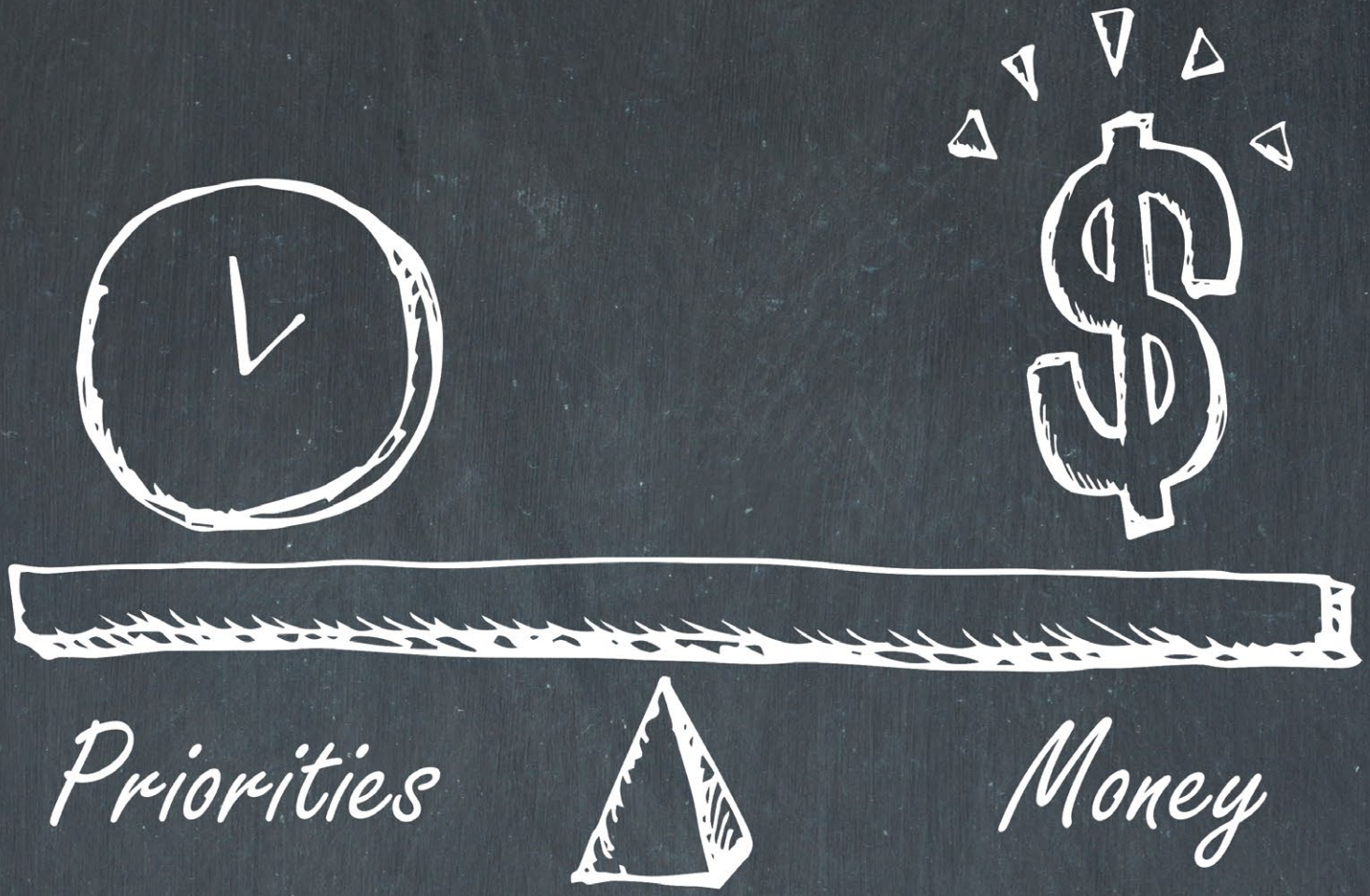
It is important to have guidelines for retention and purging of data, and MNIT can bring clarity to those guidelines from an enterprise perspective. The Records Management Statute[33] dictates that records be disposed according to a records retention schedule approved by the head of the entity and the records disposition panel, and MNIT can work toward standardizing those retention schedules across agencies and communicate them.

---

31 Examples of related data sharing initiatives across the United States can be found in Appendix K, State Chief Data Privacy Officer Background and Examples.

32 The Commission on Evidence-Based Policymaking (CEP), *The Promise of Evidence-Based Policymaking, September 7, 2017,* https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf (accessed May 24, 2020).

33 Minnesota Legislature, Office of the Revisor of Statutes, Minnesota Statutes, Section 138.17, https://www.revisor.mn.gov/statutes/cite/138.17 (accessed May 24, 2020).



Section 7

Section 7

Funding

Successfully implementing and managing information technology investments so that they continue to meet customer and business needs both operationally and securely requires adequate funding for both initial and ongoing investments. These include investments for defining business and system needs, project and change management, security planning and training, development, implementation, and maintenance. Without these ongoing investments, the state creates the potential for untimely disruptions of public services, internal control and accountability weaknesses, and vulnerabilities to cybersecurity attacks. It is important to note as we enter a period where the state budget outlook is contracting that costs for ongoing maintenance and investment to upgrade technology systems are not easily reduced unless the business need changes. An example of such a business need change would be the reduction of demand for certain services.

Obtaining the funding for planning, developing, implementing, maintaining, and upgrading existing systems has been an ongoing challenge for state agencies either through the legislative process where estimating the investment cost and delivery dates have been difficult or through grants that fund the initial development of a technology application but not the ongoing costs. Moreover, there has not been consistent guidance on developing and prioritizing the ongoing system investment needs when developing, requesting, and prioritizing changes to agency operating budgets through the state budget development process. This leaves those systems and applications vulnerable to service disruptions, cybersecurity attacks, and obsolescence. Many systems are decades old using technologies that are outdated, costly, and difficult to continue supporting.

The state needs a **consistent and long-term IT funding strategy** that supports the delivery of effective, efficient, and secure systems to its partners and most importantly to 5.5 million Minnesotans. Over the last year, there were frequent conversations regarding underfunded system support needs, particularly for system modernization and routine system maintenance and upgrades that are needed to ensure cybersecurity and application support. Continuing the conversation to address enterprise investment allocation and distribution process and policies would be a good start for the BRC-IT going forward.

MNIT and agency leaders continuously update plans to improve, retire, or replace existing information technology systems to enhance cybersecurity and to improve efficiency and effectiveness across the life of a given workload. State leaders need to recognize the role these investments play in delivering quality services to the public and maintaining accountability for state government programs when competing with other funding priorities. Providing adequate, risk-based, and cost-effective IT capabilities that address evolving threats requires additional and continuous funding.

Agency Funding Challenges

The State of Minnesota's budget, like the programs it funds, is diverse. There are over 100 agencies providing services that receive funding from a variety of sources organized in nearly 200 discrete funds. The state's general fund is the largest with 55% of the state's total revenues. The second largest fund is the federal fund, which holds

the revenues from grants, reimbursements and cooperative agreements state agencies have with the federal government. There are many other accounts in the state budget containing revenue that comes to the state for dedicated purposes, such as hunting and fishing licenses at the Department of Natural Resources.

Some of these many funds have standing authority for state agencies to spend from, while others require legislative action to specifically appropriate resources, such as the general fund. Agencies pay for IT services from their dedicated statutory appropriations and through direct appropriations from the legislature. Where federal grants are available, they tend to fund IT systems as part of larger program objectives and are typically funding the planning and development of a specific application. IT projects are also funded through these mechanisms, or with the Odyssey Fund, a special revenue fund that allows agencies to transfer – after legislative approval – unspent operating funds to carry forward past the end of the biennium to be spent on IT activities that create government efficiencies.

One source is not inherently better than the others; however, except for the general fund, each fund must be spent on the specific program or service it supports. Grant funding often contains specific requirements that constrain those resources to be used specifically for the purpose for which it is intended. This can **restrict the use of common or shared system infrastructure** depending on the application design and grantor requirements. Accepting restricted grant funding in some cases limits solution options and may prevent usage of modern IT, like cloud-based infrastructure. It is important to understand the limitations and evaluate the total cost of ownership that would result from accepting the grant against the use of other funding.

The state operates on a biennial budget passed by the Legislature. The **two-year budget cycle** can present planning challenges for IT project funding. First, changes in technology can take a long time to develop, implement, and precisely forecast the total costs. Agencies generally have only one opportunity, or "one bite at the apple", to secure funding for an IT investment during a legislative session, and it is difficult to accurately estimate the correct project and ongoing maintenance and operating costs. When funding is secured, it may not be adequate to support maintenance for updates particularly with grants that often fund the initial design and development costs but do not fund the ongoing costs or where legislative proposals did not fund those costs.

Because appropriations typically do not increase beyond the two-year biennium, **funding often does not take modernization, operational increases, enhancements, or changes in software licensing costs into account.**

Similarly, for IT services, state agencies and MNIT work closely to forecast the anticipated consumption of standard IT services, like workstation, service desk, and hosting and storage, and the associated budgetary impact for the two-year period.

MNIT charges agencies for their services in two ways:

1. MNIT passes through the direct costs of agency-specific IT services for applications, software and projects that are consumed uniquely by that agency, as well as for the staff that support them. The agency gets a bill at cost and these services are not consumed by the enterprise as a whole. For example, MMB pays a pass through charge back to MNIT for the software and staff costs that support the statewide accounting system that MMB is responsible for managing.
2. MNIT charges agencies rates for services that are consumed by every agency and provided centrally by MNIT. Examples of rate-based services include desktop, laptop, workstation support, storage and backup, and connectivity.

State and federal law and policies require MNIT's rates to be set as close to the break-even level as possible and that each fund and program is charged for the service it consumes – no more or less. Therefore, rates are not a tool MNIT has to drive innovation by charging lower rates to incentivize adoption of technology that will enhance government efficiency. And, because of these restrictions, rates are also not the best tool for simplifying how the state pays for IT.

Second, funding through the legislative process needs structure and clear expectations for legislators and agencies, especially for system modernization efforts where the commitment is high, and the solutions are not well-defined at the point when funding is proposed. There are also the expectations that are set for system delivery schedules. These are also difficult to project at the point where funding is requested. This leads to scope, schedule, and resource challenges for major initiatives.

Agencies need to improve, retire, or replace existing information technology systems and increase cybersecurity efficiency and effectiveness to stay ahead of evolving information security threats. Planning for full life-cycle funding should be included in all projects with a way to ensure proper funding through the life of the application.

The existing funding model may not be compatible with implementation of the modernization principles and the Modernization Playbook. For successful adoption of both, MNIT and agencies must revisit the current funding model and identify opportunities to reduce complexity and increase incentives for modernization and improved cybersecurity.

21. Agency and MNIT leaders should review the Modernization Playbook and identify strengths, weaknesses, and capability gaps in the current staffing, processes and technology for each agency, and submit to MMB, for consideration by the Governor through the state budget development process, the changes to current funding needed to address these gaps.

Cybersecurity Funding and Critical Infrastructure

In addition to the review of IT funding generally, the BRC-IT notes a special need to reconsider funding for cybersecurity. Minnesotans need to trust that all systems are protected from cyber threats to ensure protection of their data. This is as important as transportation systems, energy, communications, water, and emergency services.

In December 2019, EmiSoft, a malware software company, released a report about ransomware attacks[34] and noted that in 2019 the U.S. was hit by an unprecedented and unrelenting barrage of attacks that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion.

34 The State of Ransomware in the U.S. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

The impacted organizations included:

- 113 state and municipal governments and agencies.
- 764 healthcare providers.
- 89 universities, colleges and school districts, with operations at up to 1,233 individual schools potentially affected.

This level of safety and business disruption will continue to rise as the hackers add business practices to their growing enterprise of intrusion into the security of systems and theft of valuable data. A list of cybersecurity incidents can be found in Appendix N.

Cyber attacks will continue to evolve, and a designation of cybersecurity as critical infrastructure declares the physical and virtual systems are vital assets to the state, and their incapacity and destruction would be debilitating on the physical, economic, public health, and safety of our citizens. Such a designation would fit well within the framework established by the National Institute of Standards and Technology (NIST) and U.S. Department of Homeland Security. A list of federal critical infrastructure Sectors can be found in Appendix O. To ensure cybersecurity protection for the state it would include the Executive Branch, Judicial System, state government, municipalities, and tribal nations.

Based on national cybersecurity critical infrastructure declarations, cyber protection should be recognized as critical infrastructure in Minnesota to align with frameworks established at NIST. This will allow state systems to be eligible for disaster relief funding during declared emergencies. The costs for recovery of infrastructure and data are in the multi-millions of dollars for recent cyber-attacks in cities such as Baltimore, Atlanta, Houston, Pensacola, and New Orleans to name a few. These attacks significantly impact citizens' lives by preventing them from accessing services and by compromising their data privacy, while also creating a significant loss in revenue for the state. The costs to mitigate and repair far outweigh the costs to protect our citizens and systems in the State of Minnesota.

22. Cybersecurity protection should be declared critical infrastructure to allow for alternative funding capabilities, protection of operations, and expeditious responses to emergencies.

This protection would enhance the cybersecurity of state infrastructure; facilitate public and private consultation; establish frameworks for implementing cybersecurity minimum standards; and, maintain a cyber environment that encourages efficiency, cost effectiveness, innovation, and economic prosperity while also promoting safety, security, civil liberties, and privacy rights.

During the 2019 legislative session, MNIT received $20M to further cybersecurity efforts over the next four years. The funding will allow MNIT to, among other cyber investments, deploy cybersecurity tools that improve detection and blocking of attacks, create training that will help state employees spot phishing emails, and improve response time and awareness of cyber threats.

23. The Legislature should ensure that the state has long-term, consistent, predictable, and appropriate funding for cybersecurity operations, based on a percentage of the total state IT budget.

Cybersecurity operations includes contract support, maintenance, replacement, and new purchase(s). Most states' enterprise IT budgets[35]

35 NASCIO, Dedicated Cyber Funding Report, 2020, https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

allocate between 0% and 3% for cybersecurity. By comparison, private corporations allocate an average of 10% of their IT budgets to cybersecurity. State budgets have not kept pace with the needs of the current environment and evolving challenges. Legislation was introduced in 2019 with House File 2524[36] to create an Information Technology and Cybersecurity Account and dedicate 2% of all fees collected by the secretary of state by law to use for costs related to the maintenance and enhancement of the secretary of state's (1) information and telecommunications technology systems and services, and (2) cybersecurity capabilities.

Minnesota cannot fail on comprehensive cyber protection on behalf of its citizens. MNIT must provide support to agency leaders who are making decisions that impact cybersecurity, ensuring this is not an afterthought. There is a need to ensure cyber protection and increase resiliency to the advancing cyber threats and provide adequate disaster recovery systems. This requires investing in long-term operational and maintenance funding. Without a direct and long-term funding source, information security capabilities and disaster recovery will suffer, thus reducing resiliency for the State of Minnesota.

MNIT established the Application Recovery Directive in late 2019 to enhance disaster recovery efforts on applications used to support the state's life, safety, security, public health, and health care service functions. This directive supports Executive Orders 19-22 and 19-23[37] and presents an opportunity for MNIT to establish plans and coordinate the response to how the State of Minnesota addresses disaster recovery of critical IT applications from technological or natural disasters, and in particular current cyber threats. MNIT's focus is to ensure all disaster recovery plans align with the priorities and recovery timelines of our state agency partners' priority services to ensure the state is adequately managing the risk of system and service interruptions. Current disaster recovery efforts are monitored in an extensive excel spreadsheet.

An attack on a Priority 1 application would have a crippling effect on the business such as when data is unrecoverable, corrupt or lost or a server has failed and degraded to an unusable level. An attack on Priority 2 application would significantly impact the business such as when degraded application performance has a serious negative impact on business. The BRC-IT recommends continued action.

24. MNIT should expand the Disaster Recovery Roadmap to include critical applications defined as Priority 1 and Priority 2 and support additional funding to complete cloud-focused recovery capabilities for stability, data protection, and resiliency for critical systems and applications.

An efficient disaster recovery roadmap that is integrated with application health monitoring and mapping features will allow MNIT to manage time sensitive disaster recovery and plan for more data driven modernization efforts.

36 The full text of HF2524 is in Appendix F and available at https://www.revisor.mn.gov/bills/status_result.php?body=House&session=0912019&author1%5b%5d=41957&legid1=15441.

37 The full text of Executive Order 19-22 Assigning Emergency Responsibilities to State Agencies and Executive Order 19-23 Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans are available in Appendix P.

Section 8

Section 8

Conclusion

The Governor created the Blue Ribbon Council on Information Technology (BRC-IT) at a time of transition for Minnesota IT Services (MNIT), and the Chair and members have played an active role in key activities, with decisions about MNLARS and the selection of the new CIO, Tarek Tomes, as prime examples. The BRC-IT fosters strong relations between MNIT and the Governor's office, the Legislature, counties, and the private sector. This report and the quarterly reports before it are representative of the broad-ranging perspectives of the members and the many guests who contributed to the conversations. Strong attendance by members – at more than twice the meetings they originally agreed to attend – and a collaborative model made it a highly productive group. It is evidence that a small group of passionate people who are good listeners and offer varied insights can truly make a difference.

Acting on all the recommendations in this report will establish a firm foundation for modernization success and secure systems. There will be much more discussion on the topics above in the months to come – and on other actions not yet identified.

As was seen by the work on the MNLARS review and replacement, the state and its agencies have the ability to do great things but often hesitate. The hesitation and other factors cause a loss of precious time to fix problems. We need to cultivate an environment where we move fast and boldly with fact-based solutions to our pressing IT issues, which often are more business problems than IT problems. We must work hard to reimagine how we deliver our services and then use technology and automation to provide these services. The main point is to focus on the business process before introducing technology. Just because we've done it a certain way for years is no reason not to revisit it. Additionally, third-party, off-the-shelf software often is available and will get us 90% of what we want. All we must do is adapt the business processes in the last 10% to make use of the software.

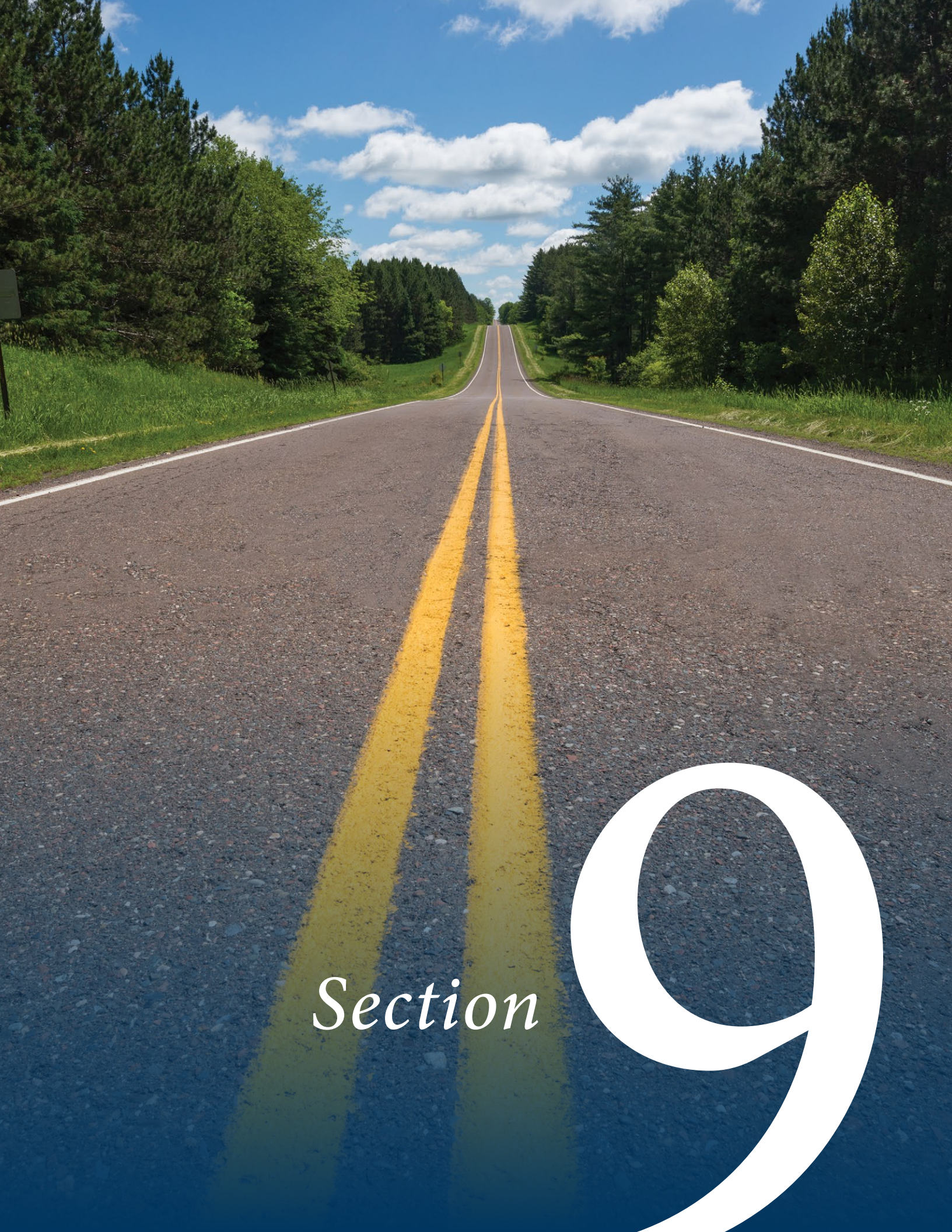
The recent performance of MNIT staff in response to Covid-19 is something to be thankful for. This unprecedented situation paved the way for decisions and behavior that were not previously possible or seen. In some cases, challenges to ideas simply fell away, as in the case of the Skilled Professional Program. The state proved that it can act swiftly to leverage outside experts. The lessons of this experience must not be missed, and progress made must not be lost.

Recognizing that Covid-19 is going to significantly impact the state budget and that legislators and agency leaders will have to make tough choices about what gets funded and what gets prioritized, the BRC-IT encourages all to remember that IT modernization is not an optional activity that can be indefinitely postponed. It is not simply a cost of doing business. It is an investment in the delivery of services that Minnesotans want and deserve.

The BRC-IT is grateful for:

- The strong support and perspective of the Governor and the agency commissioners.
- The active participation and guidance from the legislative members, Senator Melissa Wiklund, Senator Mark Koran, Representative Kristin Bahner, and Representative Jim Nash.
- The lessons shared by MNIT staff, county representatives, and private-sector experts.
- The many guests, including presenters from agencies and private companies, as well as regular attendee and contributor Representative Steve Elkins.
- MNIT leadership for welcoming all ideas, engaging in working sessions, and quickly responding to requests for information.

With the steady leadership in place at MNIT, strong support from the Governor and agency commissioners, and the new, revised Technology Advisory Council working collaboratively for reform, we can create a new normal for IT Services for the State of Minnesota.



Section 9

Section 9

Future BRC-IT Topics to Explore

Many of the topics discussed during the first year of the BRC-IT will continue to be important in discussions about Modernization, Cybersecurity, and Data Management and Privacy.

In the recommendations in this report, the BRC-IT requested that plans be developed for the following topics and presented to the council:

- Cataloging data.
- Real-time portfolio reporting.
- Measuring performance against the Modernization Principles and Playbook.
- Technology and cybersecurity education.
- A Skilled Professional Program.
- A public/private partnership for cybersecurity.
- Creating Modernization Outlooks with agencies
- Changing the funding model for IT.
- Expanding MNIT's role in coordinating IT governance, with support from executive and legislative branches.

There will certainly be other topics raised for discussion as well, but the BRC-IT proposes the following for ongoing research and conversation.

- Disaster recovery and business continuity.
- Data management and governance, including cataloging data and efficient use and reuse and sharing of data.
- An examination of consumer technologies and how they may be broadly embraced as part of a state-wide consumer engagement technology strategy.

Some discussions are already well underway, and others are just getting started. In either event, the BRC-IT can continue to monitor progress and offer feedback that takes into consideration the needs of Minnesotans. It can also surface perspectives and best practices to advance IT modernization that come from the private sector and the government sector at both state and local levels, in Minnesota and in other states.

Appendices

Appendix A | Legislative Charge for the TAC

16E.036 Advisory Committee[38]

(a) The Technology Advisory Committee is created to advise the chief information officer. The committee consists of six members appointed by the governor who are individuals actively involved in business planning for state executive branch agencies, one county member designated by the Association of Minnesota Counties, one member appointed by the governor as a representative of a union that represents state information technology employees, and one member appointed by the governor to represent private businesses.

(b) Membership terms, removal of members, and filling of vacancies are as provided in section 15.059. Members do not receive compensation or reimbursement for expenses.

(c) The committee shall select a chair from its members. The chief information officer shall provide administrative support to the committee.

(d) The committee shall advise the chief information officer on:

(1) development and implementation of the state information technology strategic plan;

(2) critical information technology initiatives for the state;

(3) standards for state information architecture;

(4) identification of business and technical needs of state agencies;

(5) strategic information technology portfolio management, project prioritization, and investment decisions;

(6) the office's performance measures and fees for service agreements with executive branch agencies;

(7) management of the state MN.IT services revolving fund; and

(8) the efficient and effective operation of the office.

38 Minnesota Legislature, Office of the Revisor of Statutes, Minnesota Statutes, Section 16E.036, https://www.revisor.mn.gov/statutes/cite/16E.036 (accessed May 24, 2020).

Appendix B | Executive Order for the BRC-IT

Executive Order 19-02[39]

Establishing the Governor's Blue Ribbon Council on Information Technology

I, Tim Walz, Governor of the State of Minnesota, by the authority vested in me by the Constitution and applicable statutes, issue the following Executive Order:

The Governor and Lieutenant Governor recognize the important work done by Minnesota IT Services ("MNIT") in providing technology support and services for 5.5 million Minnesotans. MNIT's 2,300 employees work closely with state agencies to provide applications for areas ranging from health care to hiking trails Minnesota is a leader in information technology ("IT"), one of only ten states in the country to receive an A- or higher from Digital States in 2018 and ranked third for Emerging Technologies and Innovation. Nonetheless, technology is ever evolving, and new challenges and threats to our IT systems arise every day. To ensure that Minnesota's IT systems are robust, efficient, and secure, the Governor and Lieutenant Governor seek to enlist the expertise of Minnesota's best and brightest technological minds across the public and private sectors.

The Governor's Blue Ribbon Council on Information Technology ("Council") will be an advisory group to the Governor and Lieutenant Governor made up of experts on development and implementation of IT in private and public institutions. The Council will provide advice on how to update and maintain the State's IT systems to ensure that Minnesota residents and businesses who interact with the State receive the best possible service. Members of the Council will also advise on the most efficient use of taxpayer dollars invested in IT projects, while keeping government data secure and protecting the State against cybersecurity threats.

The Council expands the existing Technology Advisory Committee. The Council will include additional members with IT expertise and state legislators. The Governor and Lieutenant Governor seek advice from IT experts in the public and private sectors and from legislative leaders as the Council tackles issues of data privacy, cybersecurity and updating old state computer systems.

For these reasons, I order that:

1. The Governor's Blue Ribbon Council on Information Technology ("Council") is established.
2. The Council will provide private and public sector counsel to the Governor, Lieutenant Governor, Commissioner of Minnesota IT Services, and the Legislature.
3. The Council will be comprised of the following voting members:

---

39 State of Minnesota, Executive Department, Executive Order 19-02, https://www.leg.state.mn.us/archive/execorders/19-02.pdf, Establishing the Governor's Blue Ribbon Council on Information Technology, February 6, 2019, St. Paul, Minn.

a. Fifteen voting members:
    i. The nine members of the existing Technology Advisory Committee as set forth in Minnesota Statutes 2018, section 16E.036
    ii. Six additional members selected by the Governor and Lieutenant Governor with private-sector or public-sector IT experience or experience in academia pertaining to IT
b. Four *ex officio* non-voting members:
    i. A member of the Minnesota House of Representatives selected by the Speaker of the House
    ii. A member of the Minnesota House of Representatives selected by the Minority Leader
    iii. A member of the Minnesota Senate selected by the Majority Leader
    iv. A member of the Minnesota Senate selected by the Minority Leader

4. The Governor and Lieutenant Governor will designate one of the fifteen voting members to serve as the Council's Chair.
5. The Council will have three sub-committees:
    a. A Data Privacy Sub-Committee to provide advice related to the State's use and protection of private data and liaise with the Legislative Commission on Data Practices and Personal Data Privacy
    b. A Cyber Security Sub-Committee to provide advice related to the protection of the State's IT infrastructure
    c. A Modernization Sub-Committee to provide advice related to the State's largest and most complex IT projects
6. Each Sub-Committee will be comprised of five members of the Council, as assigned by the Council's Chair. Each Sub-Committee will appoint a Chair from its membership.
7. The Council may establish additional sub-committees as necessary to advance its work.
8. The Council will hold its first meeting in March 2019.
9. Meetings of the Council will occur every other month; Sub-Committee meetings will be held during the alternate months.
10. Sub-Committees may hold additional meetings as needed to advance the Council's work.
11. The Council will prepare quarterly reports to the Governor, Lieutenant Governor, the Commissioner of Minnesota IT Services, and the Legislature, with the first report due by June 30, 2019. The quarterly reports will provide an update on the status of the above activities.
12. Minnesota IT Services will provide staffing and administrative support to the Council.

This Executive Order is effective fifteen days after publication in the State Register and filing with the Secretary of State. It will remain in effect until June 30, 2020 or until rescinded by proper authority.

Signed on February 6, 2019.

Appendix C | BRC-IT Membership and Subcommittee Assignments

Name	Organization	Position
Rick King	Thomson Reuters	**BRC-IT Chair**
Renee Heinbuch	Washington County	**Cybersecurity Chair**
Tewodros "Teddy" Bekele	Land O' Lakes	Cybersecurity
Laurie Martinson	Dept. of Natural Resources (DNR)	Cybersecurity
Rep. Jim Nash		Cybersecurity
Sen. Melissa Wiklund		Cybersecurity
Dep. Comm. Eric Hallstrom	Management and Budget (MMB)	**Data Mgmt & Privacy Chair**
Comm. Margaret Anderson Kelliher	MN Department of Transportation (MN DOT)	Data Mgmt & Privacy
Rep. Kristin Bahner		Data Mgmt & Privacy
Jason Lenz	Lyon County	Data Mgmt & Privacy
Nancy Lyons	Clockwork	Data Mgmt & Privacy
Mike McCullough	National Marrow Donor Program	Data Mgmt & Privacy
Theresa Wise	Formerly Delta/Northwest Airlines	**Modernization Chair**
Tom Butterfield	TCF Bank	Modernization
Dep. Comm. Lee Ho	Dept. of Revenue (DOR)	Modernization
Comm. Steve Grove	Dept. of Employment and Economic Development (DEED)	Modernization
Dep. Comm. Chuck Johnson	Dept. of Human Services (DHS)	Modernization
Kasandra Church	MN Assoc. of Professional Employees	Modernization
Sen. Mark Koran		Modernization

Chair Rick King, MNIT Commissioner Tarek Tomes and the legislators (Senator Melissa Wiklund, Senator Mark Koran, Representative Kristin Bahner and Representative Jim Nash) served as ex-officio members for each of the subcommittees.

Appendix D | BRC-IT Speaker List

Month	Type	Speaker
April	Presentation	**Cybersecurity** Richard Puckett, CISO, Thomson Reuters
	Agency Overview	**Department of Human Services** Deputy Commissioner Chuck Johnson
May	Agency Overview	**Department of Transportation** Commissioner Margaret Anderson Kelliher
June	Agency Overview	**Management and Budget** Commissioner Myron Frans
July	Presentation	**Clockwork: Human-Centered Design Thinking** Micah Speiler, Director of Experience Design Danielle Miller, Experience Strategist
	Agency Overview	**Department of Revenue** Commissioner Cynthia Bauerly
August	Agency Overview	**MN State Demographer** Susan Bower
September		*Report Review - No Guest Speaker(s)*
October	Presentation	**County-State Interactions** Renee Heinbuch, IT Director, Washington County Jason Lenz, IT Administrator, Lyon County
	Presentation	**Procurement** Tracy Gerasch, MNIT Procurement Betsy Hayes, Department of Administration
	Agency Overview	**Department of Administration** Betsy Hayes, Chief Procurement Officer Rachel Dougherty, Professional/Technical Manager Luke Jannett, Acquisitions Manager
	Agency Overview	**MNIT** Tracy Gerasch, IT Procurement Director

November	Discussion	**Chief Privacy Officer and Data Practices Governance** Eric Hallstrom, Deputy Commissioner, MMB Renee Lopez-Pineda, Director, Privacy Office, Delta Airlines Laurie Beyer-Kropuenske, Director of Community Services, ADM Ellena Schoop, Enterprise Data Architect and Data Governance, MNIT
	Discussion	**MNIT Project and Modernization Funding Over Fiscal Periods** Commissioner Tarek Tomes, MMB Marianne Conboy, Executive Budge Officer, MMB Jon Eichten, Deputy Commissioner, MNIT
December		*Report Review - No Guest Speaker(s)*
January	Presentation	**MAPE** Kassie Church, MNIT and BRC-IT member representing MAPE
	Presentation	**MNIT Workforce** Deputy Commissioner Jon Eichten
February	Presentation	**Processes Around & Implementation of Packaged Software Solutions** Justin Kershaw, CIO, Cargill Rahoul Ghose, CIO, ECMC Joe Dabat, Sr. Director of Development, Land O' Lakes
	Presentation	**Department of Education's Ed-Fi Project** Jennifer Dougan, Director of the Research and Assessment Division, MDE David Reeg, Software Development Supervisor, MNIT
March thru June		*Report Drafting and Review - No Guest Speakers*

Appendix E | 2019 BRC-IT Recommendations

BRC-IT Report	#	Recommendation
September 2019	1	The BRC-IT recommends the statute authorizing the Technology Advisory Committee be amended and replaced by the current BRC-IT
September 2019	2	The BRC-IT recommends the Legislature, through the legislative coordinating committees, create two new committees – one for Cybersecurity and one for Technology.
September 2019	3	The BRC-IT recommends the Legislature and MNIT work together to determine how to leverage private sector expertise on IT policies, practices and procedures through a Skilled Professional program.
September 2019	4	MNIT creates a list of the top 10 business technology solution principles and establishes an IT architecture review board for applying those principles.
September 2019	5	Agencies evaluate and simplify business processes and rules before building, replacing or procuring new systems and make recommendations to the Legislature regarding modifications to laws and regulations.
September 2019	6	Agencies seek to leverage purchased software solutions (PSS) with appropriate customization and identify any legislative or regulatory obstacles that may not allow this.
September 2019	7	MNIT and the Department of Administration evaluate procurement guidelines, laws and regulations, present proposed changes to the BRC-IT for review, and document recommendations to enhance agency procurement decisions.
September 2019	8	The BRC-IT recommends MNIT presents a proposed plan to the BRC-IT for eventual real-time access to project and portfolio management and reporting that ensures effective communication.
September 2019	9	It is strongly recommended that legislators participate in cybersecurity training.
September 2019	10	MNIT provides senior agency leaders with education and training on IT modernization, cybersecurity risk assessment, and data management.
September 2019	11	The BRC-IT recommends data collection, maintenance, and usage be considered prior to initiation of IT development or modernization efforts.
September 2019	12	The BRC-IT recommends agencies shall, in collaboration with MNIT, identify and purge data on an ongoing basis as aligned with best practices, particularly private and nonpublic data, that is no longer necessary for agency functions or required by law to be maintained.

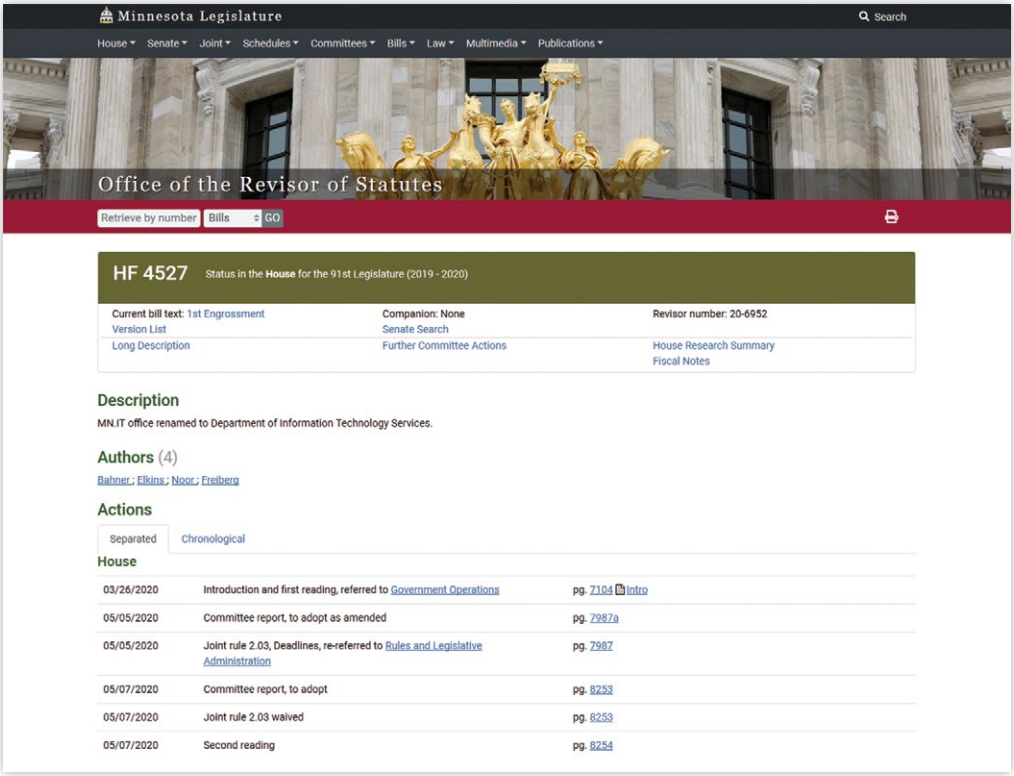
December 2019	1	MNIT and the Department of Administration should ensure that agencies understand and use their authority and ability to engage more fully with vendors before a final vendor is selected.
December 2019	2	MNIT will convene a working group that includes MNIT and other agency representation to draft and present to the BRC-IT Modernization Subcommittee a high-level Playbook for IT Modernization. It should cover the processes and responsibilities associated with business case development, process analysis, stakeholder engagement, acquisition, solutioning with vendors, talent strategy, managing change, systems operations, and system maintenance. It should ensure appropriate business process reengineering with strong stakeholder engagement.
December 2019	3	State agencies should work closely with MNIT to develop a 10-year Outlook for Business Modernization, so they can jointly create a 5-year technology modernization plan.
December 2019	4	State agencies should work closely with other governmental units (including through MNCITLA) and tribal governments as partners at the beginning of projects and include an assessment of their data needs and challenges.
December 2019	5	State agencies should include other governmental units (including MNCITLA) and tribal governments in the process of developing data privacy and management policies.
December 2019	6	The state should minimize the collection of unnecessary data on individuals (including Personally Identifiable Information, also known as PII) when developing programs, polices, and legislation, and should promote this practice in conversation with other governmental units and tribal governments.
December 2019	7	State leaders should align data definitions to facilitate data sharing and system interoperability. In furtherance of this goal, MNIT should convene a working group of MNIT and agency staff to make recommendations regarding the creation of a common data catalog and a metadata framework.
December 2019	8	Declare Cybersecurity Protection as critical infrastructure to allow for alternative funding capabilities, protection of operations and expeditious responses to emergencies.
December 2019	9	Incorporate long-term, consistent, predictable and appropriate funding for cybersecurity operations, including maintenance, replacement and new purchase(s), into the state budget, based on a percentage of total spending.
December 2019	10	Create a public/private partnership for cybersecurity to support other governmental units and tribal governments.
December 2019	11	Within the LCC Legislative Commission on Cybersecurity, include procedures for the legislators to have appropriate security clearance and to hold closed meetings for briefings on the current condition of cybersecurity for the State of Minnesota.

Appendix F | Legislation Related to BRC-IT Recommendations

Three recent bills have been introduced that relate to BRC-IT recommendations:

HF 4527[40]

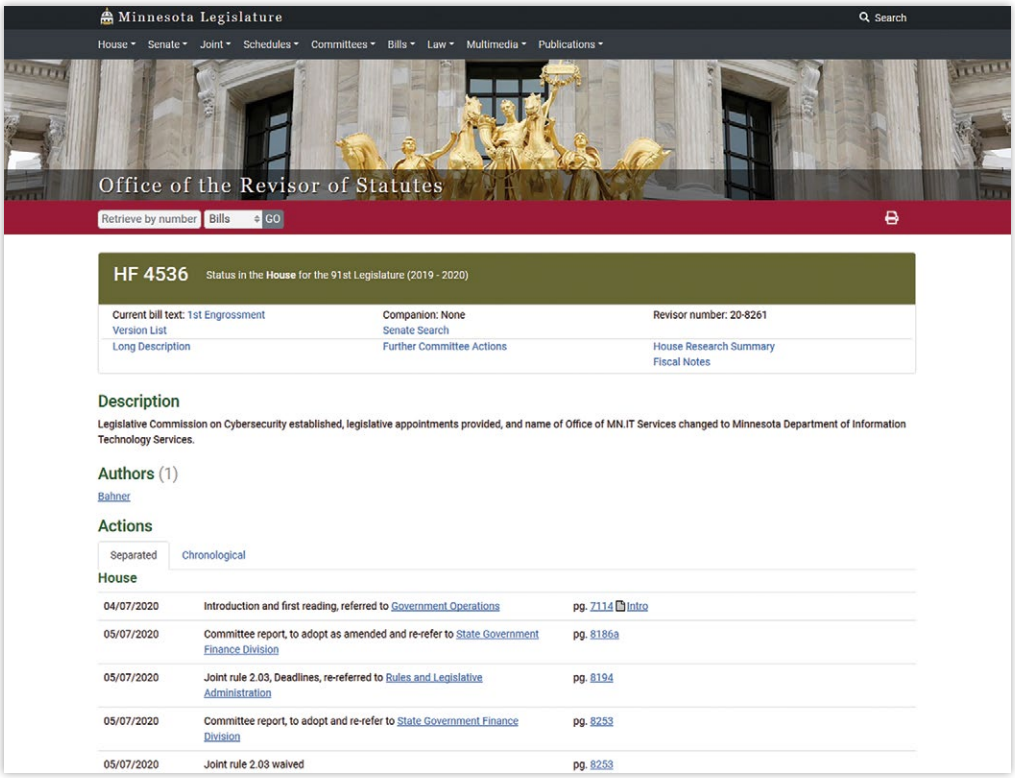
Seeks to amend Minnesota Statutes Chapter 16E, including the provision establishing the Technology Advisory Committee.



40 https://www.revisor.mn.gov/bills/bill.php?f=HF4527&b=house&y=2019&ssn=0

HF 4536[41]

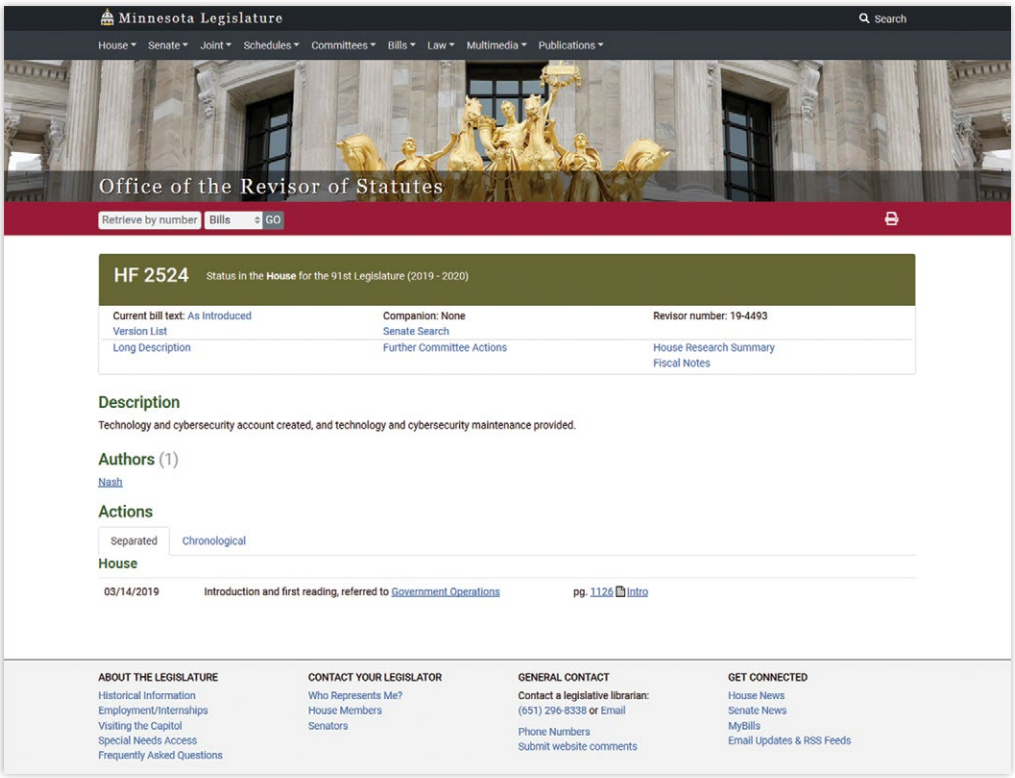
Proposes the creation of a Cybersecurity LCC



41 https://www.revisor.mn.gov/bills/bill.php?f=hf4536&b=house&y=2019&ssn=0

HF 2524[42]

Sets up the establishment of designated funding for IT and cybersecurity.



42 https://www.revisor.mn.gov/bills/bill.php?f=hf2524&b=house&y=2019&ssn=0

Appendix G | Timeline for IT Services for State of MN

Timeline of IT services, employee and finances consolidation during the two decades starting in 1996

1996
Governor Carlson issues executive order establishing an Office of Technology Coordination to coordinate the development of education-related technologies.

1997
Legislature creates a central IT agency, the Office of Technology

1999
Legislature places the Office of Technology under the Commissioner of Administration's supervision.

2003
Legislature authorizes the Department of Administration to identify opportunities for shared IT systems and services.

2005
Legislature creates an IT agency, the Office of Enterprise Technology (OET), consolidating the Office of Technology and the InterTechnologies Group.

Governor Pawlenty issues two executive orders with IT components: (1) authorizing the Drive to Excellece Initiative to create shared IT services, plans, and standards; and (2) implementing a "one-stop shop" licensing system.

2006
OET completes enterprise e-mail project, consolidating 21 e-mail systems into 1 system.

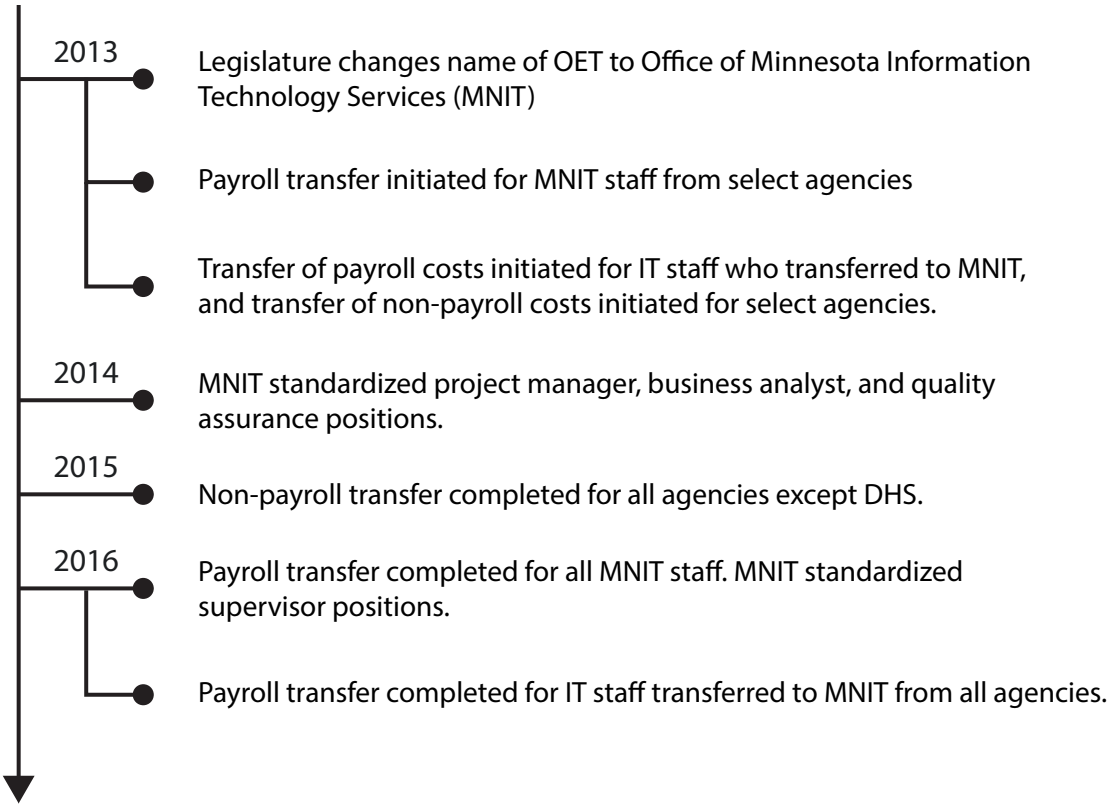
2009
Legislature creates geospatial information systems office (MnGeo), which will later become part of OET.

2010
Legislature requires study regarding consolidation of state data centers.

2011
Legislature passes IT consolidation legislation, consolidating state executive branch IT functions and staff within one agency (OET).

Agencies transferred IT staff authority to OET through interagency agreements.

2012
Agencies legally transferred IT staff to OET.


2013
Legislature changes name of OET to Office of Minnesota Information Technology Services (MNIT)
Payroll transfer initiated for MNIT staff from select agencies
Transfer of payroll costs initiated for IT staff who transferred to MNIT, and transfer of non-payroll costs initiated for select agencies.
2014
MNIT standardized project manager, business analyst, and quality assurance positions.
2015
Non-payroll transfer completed for all agencies except DHS.
2016
Payroll transfer completed for all MNIT staff. MNIT standardized supervisor positions.
Payroll transfer completed for IT staff transferred to MNIT from all agencies.

Appendix H | MNIT Guiding Principles, Tactical Plan & Priorities

Guiding Principles

Mission

We partner with Minnesota state agencies to deliver technology solutions that transform how government provides services for the people of Minnesota.

Vision

Partners in Performance – We will become the true and trusted partners for all state agencies, using our knowledge to help further the work of government.

Diversify our Workforce – We will create a workforce that includes variety of backgrounds, styles, perspectives, values and beliefs that is representative of the face of Minnesota.

Moving Government Forward – We will partner with private industry to empower our workforce to provide the best market solutions in a blended service delivery model.

Values

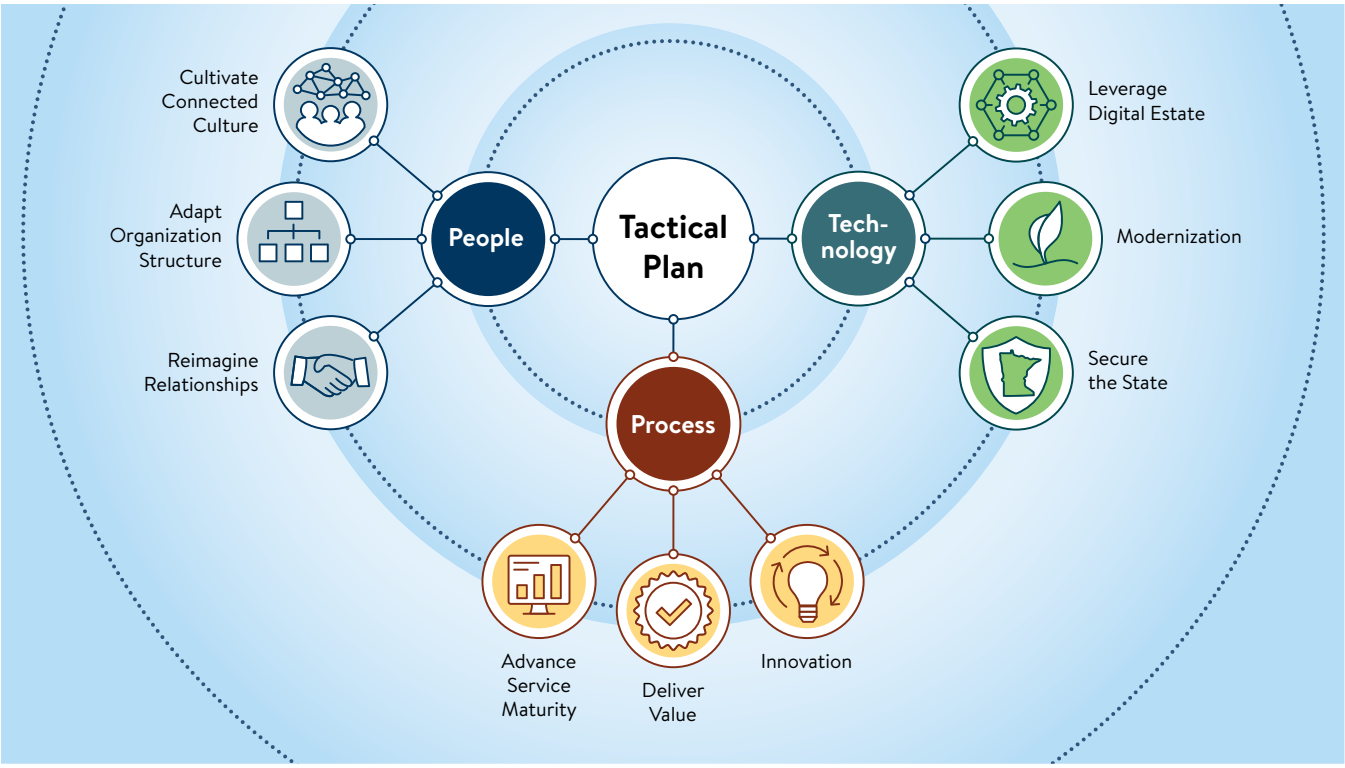
Partner – We work across our organization and with agencies to build partnerships that ensure success. Bringing together the business of state government and the complexity of technology, we provide solutions that benefit all Minnesotans.

Deliver – The pride we take in our work and the confidence we have in our expertise means we meet the promise of business value by delivering quality IT solutions on time and on budget.

Transform – We seek better ways to work. By combining the best of process and creativity, we continuously look for new ways to make government better.

Connect – We know our ultimate customer is an individual who needs our service to support themselves, their family and their work. We do not do IT for IT's sake, rather we work for those who depend on state services in their daily lives.

MNIT Tactical Plan



MNIT Top Priorities

Secure the State

Minnesota is charged with protecting data and applications against external and internal threats. Information security is one of our top priorities, and we strive to build security into every system and application that we support across the State of Minnesota. Advanced attacks are becoming more sophisticated and more common, testing the limits of existing capabilities.

- **Implement the security foundation.** MNIT will apply its security foundation for the executive branch of state government. We will work with our partners to build security into every system and application in Minnesota and invest aggressively to better protect citizens' data.
- **Empower business and promote collaboration.** Minnesota IT Services will provide leadership to other levels, units, and branches of government, and implement governance to make all Minnesota government entities more secure. It is critical that state leaders work together to address the increasing barrage of advanced and persistent threats.
- **Improve Minnesota's cybersecurity workforce.** Both public and private sector organizations are scrambling to attract and retain cybersecurity talent. We will partner with Minnesota's colleges and universities to promote careers at the state.

Modernization: Empower Our Business Partners through Technology

Many of our systems are becoming increasingly costly to maintain, are at technological risk, and no longer meet business needs. Risks, costs and complexity of these systems compound each year. As more than 1,600 applications reach the end of life, we must work together to refresh and reinvest on a regular basis. Minnesota has the responsibility to not only upgrade technology, but to invest in renewing the process of how government conducts business and to leverage existing technology, where possible, to solve broader problems in our state.

- **Build Understanding.** To make smart investments in modernization, Minnesota must fully understand the scale and scope of outdated IT systems and business processes. It is important for all state leaders to understand the risk and recognize that modernization will carry significant costs.
- **Take Inventory, Analyze and Map the Problem.** MNIT will address substantial gaps found in agency technology environments by seeking funding for basic level needs and modernizing when risks and funding come together.
- **Transform from "Current State" to "Future State".** MNIT must work with leaders across the state to invest strategically while constantly watching for opportunities to improve how we deliver services for Minnesotans.

Deliver Value: Provide Excellent Customer Service

MNIT must make decisions at every level of our organization with our customers in mind. We will leverage the state's information technology portfolio, take into account industry best practices, and promote enterprise business and technology solutions where we can provide excellent customer service to both solve business needs and maximize the benefits of shared services.

Customer-Focused Delivery. MNIT is measured by how well we successfully deliver for the State of Minnesota, and how well things are working for Minnesotans. We will work to improve communications, build cooperation, and facilitate engagement with our partners.

More Customer Feedback. We will use our Governance Framework to ensure that feedback from our agency partners is incorporated into the services that we provide and that the cost of the service is transparent. Our partners will help us determine if a service should be delivered for the enterprise or locally due to highly customized business needs.

Enhanced Enterprise Services. MNIT will continue to improve enterprise service delivery by bringing teams together to deliver standardized services using industry best practices in all of the IT services we provide.

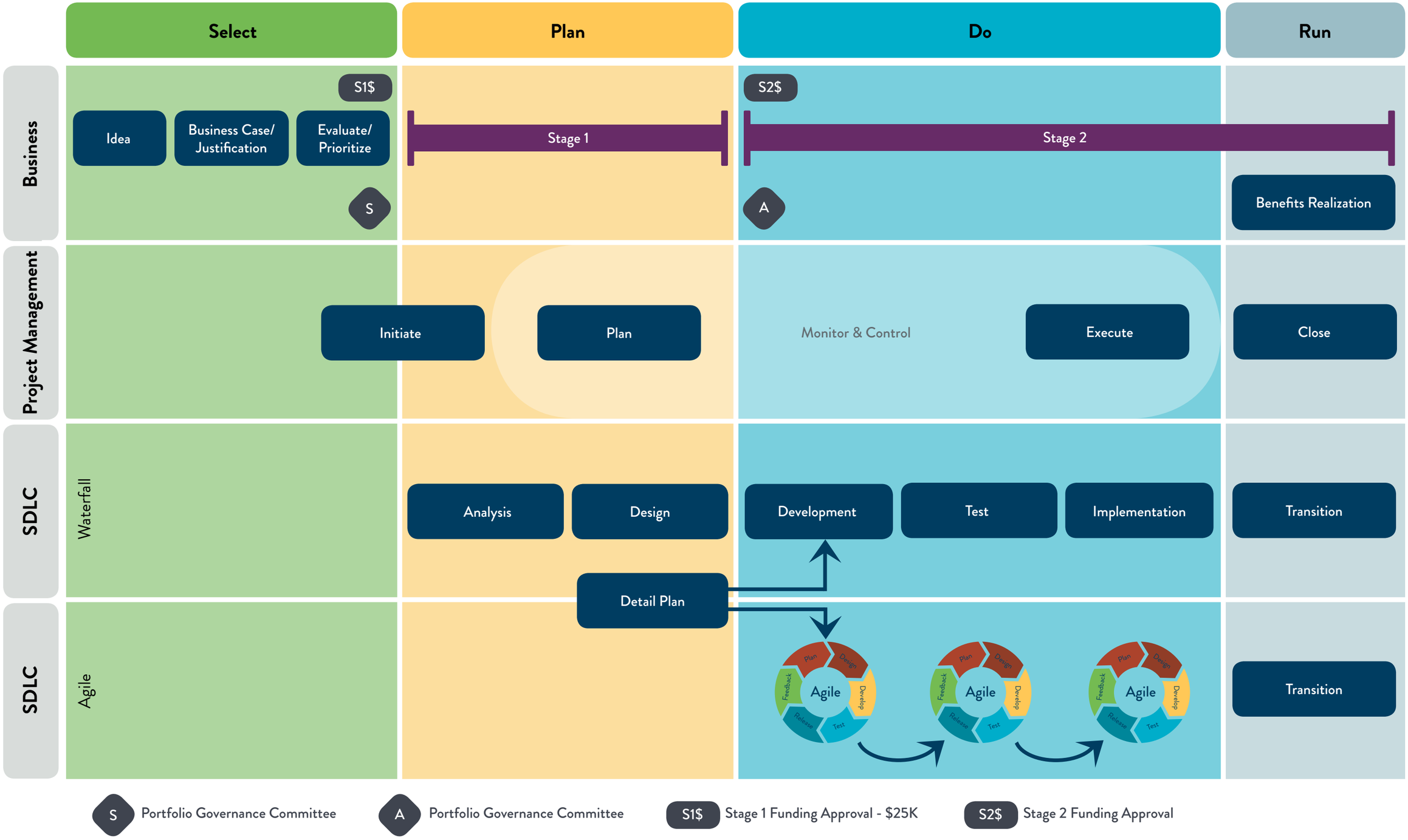
MINNESOTA IT SERVICES

Modernization Playbook

	Select			Plan	Do		Run		
	Define Problems and Opportunities	Solution Strategy	Procurement Strategy	Project Planning	Execution	Launch	Closure	Operations/ Maintenance	Application Portfolio Management
	Approve Concept			Approve Business Case First funding stage: Dollars to plan project	Approve Project Plan Second funding stage: Dollars to execute project				
Business Goal/ Outcome	Identify Org. pain points and opportunities that would drive modernization efforts (e.g. program integrity, productivity, service accessibility, tech risk, etc.)	Identify potential business process changes and potential technology solutions.	Determine strategy for procurement of necessary resources and tools.	Develop a detailed course of action or path to successfully complete the project.	Develop the product or service and present the final product to the customer for acceptance	Launch the working software solution and associated business process changes.	Finalize project activities & transfer completed project to operations.	Ongoing operational support based on agreed to service levels.	Roadmap & plan for the future of this application solution.
Key Questions and Considerations	• What are your pain points? • Who are our stakeholders? • What are key metrics that define Org. success?	• What is the desired business functionality? • Are there any constraints that may limit the solution options?	• Are there budget/timing considerations? • Are there immediate needs for current system?	• What budget, schedule, or resource constraints? • Who needs to review/approve decisions? • How will the stakeholders be involved? • Are there dependencies on other projects? • What methodology will be used to manage the project? Agile? Waterfall? Or Hybrid?	• Are we tracking to plan? • Is work output aligning to stakeholder acceptance criteria? • Are the stakeholders included in testing & acceptance?	• Who will be involved in the launch decision? • How will the launch be communicated? • How will the release be monitored post launch to evaluate success/issues?	• How did the actuals compare to our plan? • What lessons learned can apply to future projects? • Were the promised benefits realized?	• What is the plan for future releases & patching? • Are system operating risks managed appropriately? • Are we in compliance with licensing & contracts?	• How does the system align with tactical & strategic technology goals? • How is stakeholder satisfaction measured?
Activities	• High-level SWOT • Ideation Sessions on mission/vision, challenges and opportunities • Stakeholder surveys	• Market & peer research • Assess the maturity of the Org. (IT & Business processes) • Define high level requirements • Specify integrations • Determine budget	• Business case review • Initial planning meeting(s) • Engage SMEs • Engage vendor community (depending on strategy)	• Define and sequence tasks • Create budget • Identify resources (staff, skills • Detailed requirements and acceptance criteria definition • Detailed architecture and design definition • Elicit requirements	• Coding/configuring systems, data migration and building interfaces • Iterative testing and stakeholder acceptance • Schedule, Issue and Risk Management • Release planning • Status reports	• Release readiness checking, scheduling & validation • Verify and document backups, security plans, monitoring, DR plans • Manage Go-No-Go documents, communications	• Perform project review • Validate acceptance • Confirm delivery of objectives & benefits • Review action items & note transition and/or resolution • Close contracts • Evaluate vendors	• Execute transition from delivery to M&O staffing and work plans • Train O&M team • Implement performance metrics	Manage ongoing operations and support of application
Roles	• Executive Leadership • Service Delivery Leaders (division directors) • Product owners • CBTOs	• Executive sponsors • Service delivery leaders • SMEs • Stakeholders	• Procurement Analyst (“Navigator”) • Stakeholders • Agency General Counsel(s)	• Project manager • Business analyst • Quality analyst • ScrumMaster	• Project manager • Business analyst • Quality analyst • ScrumMaster	• Project manager • Business analyst • Quality analyst • ScrumMaster	• Project manager • Business analyst • Quality analyst • ScrumMaster	• Product Owner • Executive Sponsor(s) • Project SMEs • Stakeholders	• Product Owner • Executive Sponsor(s) • Project SMEs • Stakeholders
Deliverables	Problem/situation statement	Business Case	Solicitation documents: RFI, POC, RFP	Project planning documents to include: Project scope, acceptance criteria, schedule, budget, requirements and traceability matrix, risk management plan, tech and design spec, functional spec, and functional testing scripts	Tested and accepted solution	• Launch Go/No-go decision • Communication plan for stakeholders	• Project close report • Lessons learned document	• Product plan • Application health targets	• Ongoing Application performance assessment • Application Roadmap

Define the change	Plan the change	Implement the change	Sustain the change	Benefit from the change

Organizational Change Management


Select
Plan
Do
Run
Business
S1$
Idea
Business Case/ Justification
Evaluate/ Prioritize
S
Stage 1
S2$
Stage 2
A
Benefits Realization
Project Management
Initiate
Plan
Monitor & Control
Execute
Close
SDLC
Waterfall
Analysis
Design
Development
Test
Implementation
Transition
Detail Plan
SDLC
Agile
Plan
Design
Develop
Test
Release
Feedback
Agile
Transition
S Portfolio Governance Committee
A Portfolio Governance Committee
S1$ Stage 1 Funding Approval - $25K
S2$ Stage 2 Funding Approval

Appendix J | MNIT ePMO Dashboards, Current State and Future State

Current

IT projects with a total expected cost greater than $1M are registered into MNIT's Enterprise Project Portfolio Management (PPM) tool. Registered information includes project description, objectives, timelines, risks, issues, and budget. Information from the enterprise PPM tool is aggregated, summarized and extracted for reports to MNIT senior leadership and the Legislature.

The IT Project Portfolio Summary is one report produced for the Legislature as required by statute with key facts on the Enterprise Project Portfolio including: agency, timelines, summaries and project health. MNIT quarterly reports provide a quarterly summary review of projects comprised of quantifiable results, graphical summaries and narratives on notable projects. Quantifiable results include the total number of projects, the number of projects started and completed over the quarter, and a breakdown of the project count by business value. Project count by businesses value is also depicted graphically. The business value is as follows: project addresses audit finding, fulfills a legislative mandate or federal requirement, creates a solution to make support and/or delivery of business functions more efficient and effective, secures information assets, and improves enterprise IT service deliver, reduces cost for IT service, or retires/replaces aging system. IT Project Portfolio Management is performed at the agency-level where CBTOs actively partner with agency leaders to intake, evaluate, approve, and monitor projects. Project prioritization at the agency levels ensures alignment with agency mission and vision.

Future

MNIT is advancing towards real-time based with reporting and recently launched an ePMO Dashboard that collects the valuable information gathered from agency-level project portfolio management into a tool that provides real-time updates to MNIT leaders. These real-time updates will help to identify risk earlier in the project lifecycle. Whether risk results from project complexity, funding, resource management issues, ePMO is working on assessment tools to identify and mitigate risk earlier in order to keep projects on schedule and to make proactive course corrections. The agency-level project portfolio management processes will likely continue as those MNIT staff working alongside agencies possess a deep understanding of agency business needs. MNIT's goal is to integrate agency-level project information, through automation, into an Enterprise Project Portfolio that presents a more holistic, One Minnesota view. An enterprise-level Project Portfolio view coalesces information on technology trends, project cost and risk, and business valued added.

Appendix K | State Chief Privacy Officer Background and Examples

Private industry leads the way in installing CPOs, with the first known CPO position established in the early 1990s. The federal government provides leadership in a similar capacity through the role of the Senior Agency Official for Privacy. Increasingly, states are slowly but steadily starting to employ CPOs, as well.

According to NASCIO, the first state CPO was named in 2003 in West Virginia. The organization interviewed 12 state chief privacy officers for its publication, "Perspectives on Privacy," in March 2019. Of those 12, four had been in the position less than a year, two for less than two years, and four for less than four years.

State	Approach – Short Description
Arkansas	2017 statute created the position of chief data officer and the position of chief privacy officer to ensure the state's compliance with data privacy protections and laws
Arizona	Completed a statewide Data Sharing MOU in 2018, signed by 28 agencies, with a State Data Interoperability Council to oversee data sharing issues, establish policies and standards, and serve as a forum to air data sharing issues.
Oklahoma	Office of Management and Enterprise Services employs extensive information security policies and governance frameworks through the Data Governance Program Office; Statewide Memorandum of Understanding (eMOU).
Michigan	Executive directive signed by Governor (2013)
Colorado	State Measurement for Accountable Response and Transparent Government (SMART); Executive order established a chief evaluation officer, with the primary function to establish program and service evaluation
Connecticut	A 2014 executive order established the position of chief data officer, launched the state's Open Data Initiative, and required each state agency to designate an agency data officer, "an upper level manager with broad knowledge of agency operations and data holdings, along with an understanding of the legal and policy issues surrounding the agency's data."
Illinois	Enterprise Memorandum of Understanding (2016). Educating staff at all levels was key prior to implementation
Indiana	Indiana Performance Management Hub created as a state agency in statute with a Chief Privacy Officer
Louisiana	Chief data officer (CDO) created in 2014 after the establishment via legislation of an office technology Services with a mission of consolidating the state's executive branch IT and data services under one office
Virginia	Executive directive to conduct analysis signed by governor
West Virginia	First chief privacy officer (CPO) established in 2003 by executive order. The CPO sits in the area of the state's risk management.

Appendix L | Potential Roles and Responsibilities of the Chief Privacy Officer

There are multiple models in place for a chief privacy officer in the private and public sectors, and the roles and responsibilities vary considerably. Several of them are included in the list below. The BRC-IT believes more analysis should be done to determine which roles and responsibilities are appropriate for Minnesota.

- Create, support, and monitor a system of privacy protection across the executive branch.
- Set priorities and standard operating procedures relating to data access and data sharing agreements.
- Create privacy impact assessment, including templates, policies, and procedures around the use and monitoring of privacy impact statements.
- Ensure that agencies conduct privacy impact assessments for all IT projects (and other projects) of a certain size.
- Referee and provide final decisions for the executive branch when agency legal authorities or interpretations are in conflict.
- Conduct privacy training for agency employees.
- Work with point people or "privacy champions" in each agency to implement training and communications.
- Perform public outreach and public education functions.
- Review and advise regarding data-sharing agreements.

Appendix M | Skilled Professional Programs

Some skilled professional programs are coordinated by the beneficiary organization or governmental agency and tap subject-matter experts from multiple different companies. Other programs are coordinated by private-sector companies that deploy their own subject-matter experts out to multiple different non-profits and government agencies – or in some cases one partner non-profit. Companies interested in exploring options for impact volunteering for skilled staff and executives may wish to look at the resources available from the Corporation for National & Community Service at https://www.nationalservice.gov/resources/member-and-volunteer-development/sbv and considerations for a skills-based program included in the Stanford Social Innovation Review at https://ssir.org/articles/entry/the_promise_of_skills_based_volunteering#.

Possible benefits from these programs abound, but they have proven more difficult and complex to set up and manage than some originally thought. There must be careful planning and management for a program like this to be successful, with due attention paid to onboarding the executive and ensuring that all involved parties are clear about the need and about the services being offered.

Organization	Term	Description
Department of Homeland Security	3 months - 1 year	Ongoing program seeking U.S. Citizens in senior-level operational management or related position with extensive private sector leadership in specific functional areas 'Hard to recruit' skills and new perspectives
City of Atlanta	1 year	Short-term program utilizing a private sector executive as COO, overseeing Aviation, Fire, Police, Corrections, Parks and Recreation, Planning, Public Works and Watershed Management
City of Jacksonville	18 months	Office of Public-Private Partnerships
New Jersey Department of Children and Families	2 years	Lead and support policy development and initiatives Public-private alliance to increase public awareness of adverse childhood experiences
Starbucks & CARE	1 year	Develop a marketing campaign, serve as an executive mentor and implement a project management system
Google & Goodwill	3-6 months	Deployed technologists with skills in data analysis and AI to Goodwill to develop a national-level data strategy to understand the effectiveness of local programs.
Charlotte-Mecklenburg Schools & Bank of America	1 year	Serve as interim chief human resources officer

Appendix N | Cybersecurity Incidents

The following examples illustrate the disruption that can be caused by cybersecurity attacks, which put health, safety and lives at risk. These incidents have been recorded from around the U.S. as hackers infiltrated systems and demanded ransoms. The list is not exhaustive.

- Emergency patients redirected to other hospitals.
- Medical records inaccessible and, in some cases, permanently lost.
- Surgical procedures canceled, tests postponed, and admissions halted.
- 911 services interrupted.
- Dispatch centers rely on printed maps and paper logs to keep track of emergency responders in the field.
- Police locked out of background check systems and unable to access details about criminal histories or active warrants.
- Surveillance systems offline.
- Badge scanners and building access systems cease to work.
- Jail doors not remotely opened.
- Schools can't access data about students' medications or allergies.

Not only are emergency services impacted, other business transactions are affected as well:

- Property transactions halted.
- Utility bills not issued.
- Grants to nonprofits delayed by months.
- Websites offline.
- Online payment portals inaccessible.
- Email and phone systems cease to work.
- Driver's licenses not issued or renewed.
- Payments to vendors delayed.
- Schools closed.
- Students' grades lost.
- Tax payment deadlines extended.

Appendix O | Critical Infrastructure

Sector-specific agency

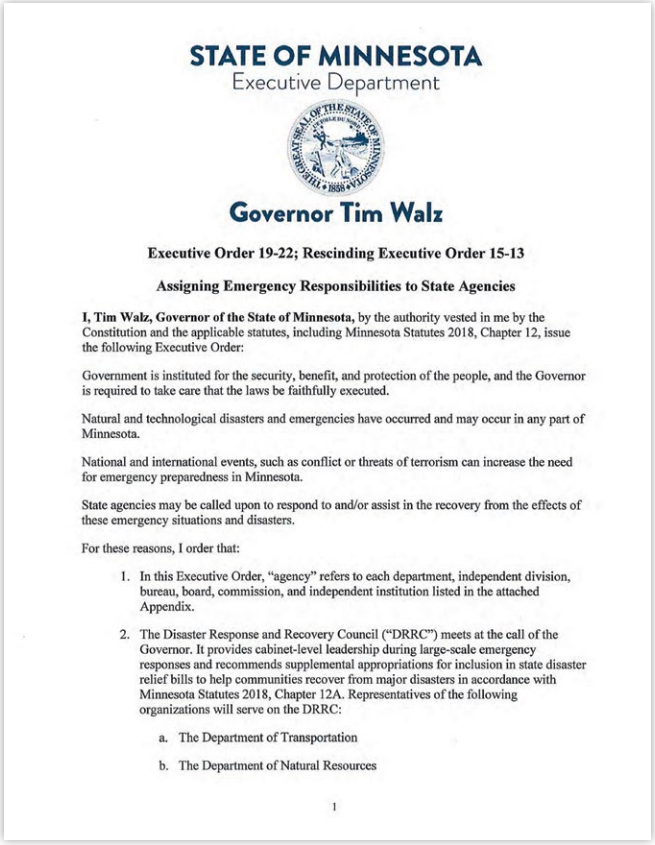
Departments of Agriculture (USDA), Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Transportation (DOT), the Treasury; Environmental Protection Agency (EPA); and the General Services Administration (GSA)

Source: GAO analysis of Presidential Policy Directive/PPD-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-19-426

Appendix P | Executive Orders related to Emergency Responsibilities and Business Continuity

Executive Order 19-22[43]

Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 15-13



STATE OF MINNESOTA
Executive Department

Governor Tim Walz

Executive Order 19-22; Rescinding Executive Order 15-13

Assigning Emergency Responsibilities to State Agencies

I, Tim Walz, Governor of the State of Minnesota, by the authority vested in me by the Constitution and the applicable statutes, including Minnesota Statutes 2018, Chapter 12, issue the following Executive Order:

Government is instituted for the security, benefit, and protection of the people, and the Governor is required to take care that the laws be faithfully executed.

Natural and technological disasters and emergencies have occurred and may occur in any part of Minnesota.

National and international events, such as conflict or threats of terrorism can increase the need for emergency preparedness in Minnesota.

State agencies may be called upon to respond to and/or assist in the recovery from the effects of these emergency situations and disasters.

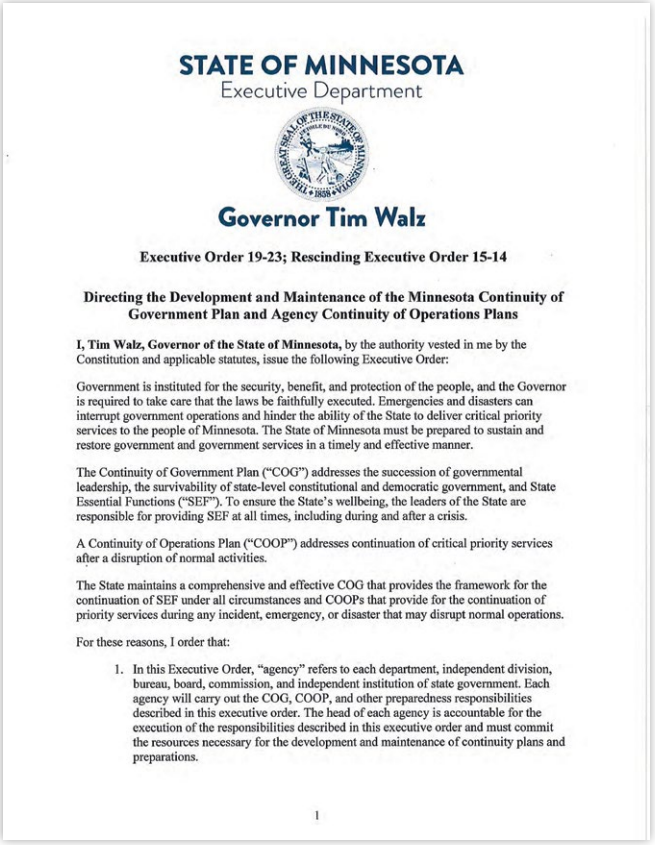
For these reasons, I order that:

1. In this Executive Order, "agency" refers to each department, independent division, bureau, board, commission, and independent institution listed in the attached Appendix.
2. The Disaster Response and Recovery Council ("DRRC") meets at the call of the Governor. It provides cabinet-level leadership during large-scale emergency responses and recommends supplemental appropriations for inclusion in state disaster relief bills to help communities recover from major disasters in accordance with Minnesota Statutes 2018, Chapter 12A. Representatives of the following organizations will serve on the DRRC:
   a. The Department of Transportation
   b. The Department of Natural Resources

1

Executive Order 19-23[44]

Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans; Rescinding Executive Order 15-14



STATE OF MINNESOTA
Executive Department

Governor Tim Walz

Executive Order 19-23; Rescinding Executive Order 15-14

Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans

I, Tim Walz, Governor of the State of Minnesota, by the authority vested in me by the Constitution and applicable statutes, issue the following Executive Order:

Government is instituted for the security, benefit, and protection of the people, and the Governor is required to take care that the laws be faithfully executed. Emergencies and disasters can interrupt government operations and hinder the ability of the State to deliver critical priority services to the people of Minnesota. The State of Minnesota must be prepared to sustain and restore government and government services in a timely and effective manner.

The Continuity of Government Plan ("COG") addresses the succession of governmental leadership, the survivability of state-level constitutional and democratic government, and State Essential Functions ("SEF"). To ensure the State's wellbeing, the leaders of the State are responsible for providing SEF at all times, including during and after a crisis.

A Continuity of Operations Plan ("COOP") addresses continuation of critical priority services after a disruption of normal activities.

The State maintains a comprehensive and effective COG that provides the framework for the continuation of SEF under all circumstances and COOPs that provide for the continuation of priority services during any incident, emergency, or disaster that may disrupt normal operations.

For these reasons, I order that:

1. In this Executive Order, "agency" refers to each department, independent division, bureau, board, commission, and independent institution of state government. Each agency will carry out the COG, COOP, and other preparedness responsibilities described in this executive order. The head of each agency is accountable for the execution of the responsibilities described in this executive order and must commit the resources necessary for the development and maintenance of continuity plans and preparations.

1

43 https://www.leg.state.mn.us/archive/execorders/19-22.pdf

44 https://www.leg.state.mn.us/archive/execorders/19-23.pdf

Appendix Q | Acronym Glossary

BRC-IT	Blue Ribbon Council on Information Technology
CBTO	Chief Business Technology Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
DAMA	Data Management Association
DGI	Data Governance Institute
DOC	Department of Corrections
DPO	Data Practices Office
DPS	Department of Public Safety
ePMO	Enterprise Project Management Office
IT	Information Technology
LCC	Legislative coordinating committee
LCPFP	Legislative Commission on Planning and Fiscal Policy
MAPE	Minnesota Association of Professional Employees
MFA	Multi-factor Authentication
MGDPA	Minnesota Government Data Practices Act
MMB	Minnesota Management & Budget
MNCITLA	Minnesota County Information Technology Leadership Association
MnDOT	Minnesota Department of Transportation
MNET	Minnesota's Network for Enterprise Telecommunications
MNIT	Minnesota IT Services
MNLARS	Minnesota Licensing and Registration System
MRB	Modernization Review Board
NASCIO	National Association of State Chief Information Officers

NCSL	National Council of State Legislators
NIST	National Institute of Standards & Technology
OET	Office of Enterprise Technology
OLA	Office of Legislative Auditor
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PMO	Project Management Officers
RFP	Request for Proposal
SWIFT	StateWide Integrated Financial Tools
TAC	Technology Advisory Committee
VPN	Virtual Private Network

Signatures respectfully submitted

Comm. Margaret Anderson Kelliher
MN Dept. of Transportation

Rep. Kristin Bahner
MN House, District 34B

Tewodros "Teddy" Bekele
Land O' Lakes

Tom Butterfield
TCF Bank

Kasandra Church
MN Assoc. of Professional Employees

Comm. Steve Grove
Dept. of Employment and Economic Development

Dep. Comm. Eric Hallstrom
Management and Budget

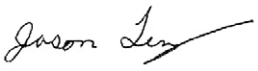
Renee Heinbuch
Washington County

Dep. Comm. Lee Ho
Dept. of Revenue

Dep. Comm. Chuck Johnson
Dept. of Human Services

Chair Rick King
Thomson Reuters

Sen. Mark Koran
MN Senate, District 32



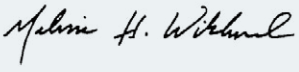
Jason Lenz
Lyon County

Nancy Lyons
Clockwork

Laurie Martinson
Dept. of Natural Resources

Mike McCullough
National Marrow Donor Program

Rep. Jim Nash
MN House, District 47A



Sen. Melissa Wiklund
MN Senate, District 50

Theresa Wise
Formerly Delta/Northwest Airlines

Letter from Commissioner Tomes

June 30, 2020

Governor Tim Walz
Lt. Governor Peggy Flanagan
Speaker of the House Melissa Hortman
House Minority Leader Kurt Daudt
Senate Majority Leader Paul Gazelka
Senate Minority Leader Susan Kent

Cc: Members of the Blue Ribbon Council on Information Technology

Minnesota IT Services is extremely grateful to Chairman Rick King and the members of Governor Walz's Blue Ribbon Council on Information Technology, for their significant contributions of time and for sharing their perspectives on how the State can better advance innovative technology services for all Minnesotans. We are fortunate to have not only some of the brightest leaders from the private sector, but also committed legislators and key government partners at the table with us. These leaders have dedicated significant time, in monthly full council meetings and regular monthly sub-committee meetings, to share insight from their years of experience as they drafted recommendations to ensure Minnesotans receive the best possible service from their state government.

The work of the Council has truly been a partnership, as we examined the role and opportunities that exist in Minnesota to ensure that Minnesota IT Services is a champion and advocate for leveraging technology as a transformative business capability. As we've heard repeatedly from our private sector members, and as we know from experience, consistent IT delivery and innovation is critical to the success of any organization – government and private-sector alike. We simply can't achieve the outcomes that government should deliver without these capabilities.

The work of the Blue Ribbon Council, and in particular the rich conversations and open dialogue we have shared, underscores the importance of a connected culture in the success of any organization. The partnerships that exist between the public and private sector, as witnessed in the work of the Blue Ribbon Council and further validated by the public–private partnerships that evolved during the COVID-19 pandemic response, are foundational for enabling innovative and transformative uses of technology to support effective government services. Such a culture must recognize the critical connections between the people we serve and the ecosystem of resources that allows us to co-create our future in the most effective manner possible.

The recommendations included in the Blue Ribbon Council's Report have been developed with these goals in mind, and MNIT is grateful for the expertise and thoughtful, consensus-driven approach that the

Council took. Minnesota IT Services is committed to advancing these recommendations in collaboration with our state agency business partners, our partners in the Minnesota Legislature, and our partners in private industry. I believe these recommendations hold tremendous promise for the executive branch and our ability to create a culture that embraces change, looks to transform the way we deliver government services through a human-centered lens, and effectively leverages the power of modern technology.

Sincerely,

Tarek Tomes

Commissioner, Minnesota IT Services and Minnesota State CIO

June 2020

This report is available in alternative formats to individuals with disabilities by calling 651-201-1118 or emailing mnit.receptioncentral@state.mn.us