SERS Retirement Board
Technology Committee Meeting
December 21, 2023
1:30 P.M.

Join Zoom Meeting
https://ohsers.zoom.us/j/92619341575?pwd=OW1pZmRLVHRWdS9sM0p3S0VraVJsUT09

Meeting ID: 926 1934 1575 **Password:** 12345

To join by phone, dial: +1 305 224 1968 and enter the Meeting ID: **926 1934 1575** and Password: **12345** when prompted.

1. Roll call
2. Approval of **September 21, 2023,** Technology Committee Minutes (R)
3. Opening Remarks
4. Executive Session pursuant to R.C. 121.22(G)(6) to discuss a security matter
5. Artificial Intelligence (AI) and SERS
6. Information Technology Update
    - Infrastructure
    - SMART
7. Risk Management and Information Security Quarterly Update
    - Quarterly Information Security Metrics
8. Upcoming Technology Committee Meetings
    - Future Topics
    - Next Meeting Date(s)
9. Adjournment

SERS Technology
Committee Meeting

December 21, 2023

_____ P.M.

Roll Call:

James Rossler _____

Frank Weglarz _____

Daniel Wilson _____

Matthew King _____

APPROVAL OF MINUTES OF THE TECHNOLOGY COMMITTEE MEETING HELD ON

September 21, 2023

_____ moved and_____seconded the motion to approve the minutes of the Technology Committee meeting held on **September 21, 2023**

Upon roll call, the vote was as follows:

ROLL CALL:	**YEA**	**NAY**	**ABSTAIN**
James Rossler	_____	_____	_____
Frank Weglarz	_____	_____	_____
Daniel Wilson	_____	_____	_____
Matthew King	_____	_____	_____

School Employees Retirement System	TECHNOLOGY COMMITTEE MINUTES		
Preparer	Megan Robertson	**Meeting Date**:	September 21, 2023
Committee Chair	Matthew King	Committee roll call was as follows: Matthew King, James Rossler, Frank Weglarz, Daniel Wilson **Also in Attendance:** SERS Staff Members: Joe Bell, Jay Patel, Jeff Davis, Joe Marotta, Richard Stensrud, Karen Roggenkamp, Vatina Gray, and Megan Robertson. Board members: Aimee Russell. Representative of the Ohio Attorney General, Lisa Reid. Guests attended virtually on Zoom.	
Agenda	1. Roll call (R) 2. Approval of July 20, 2023, minutes (R) 3. Technology and Information Security Comments 4. Technology Roadmap – Progress Updates o MVVM Upgrade 5. Information Security Quarterly Update o Artificial Intelligence – Progress Update 6. Executive Session pursuant to R.C. 121.22(G)(6) to discuss security matters 7. Upcoming Technology Committee Meetings o Future Topics o Next meeting Date(s) 8. Adjournment		
Discussion	The SERS Technology Committee meeting began in open session at 1:00 p.m. **Roll Call** The SERS regular Technology Committee began with a roll call. The committee roll call was as follows: Present: James Rossler, Frank Weglarz, Daniel Wilson, Matthew King. Also in attendance were SERS Staff Members: Joe Bell, Jay Patel, Jeff Davis, Joe Marotta, Richard Stensrud, Karen Roggenkamp, Vatina Gray, and Megan Robertson. Board members: Aimee Russell. Representative of the Ohio Attorney General, Lisa Reid. Guests attended virtually on Zoom. **Approval of Minutes** Frank Weglarz moved, and James Rossler seconded the motion to approve the minutes of the Technology Committee meeting held on July 20, 2023. Upon roll call, the vote was as follows: Yea: Matthew King, James Rossler, Frank Weglarz, Daniel Wilson. The motion carried. **Technology & Information Security Comments** SERS Deputy Executive Director, Karen Roggenkamp, provided a brief introduction of the meeting agenda. Ms. Roggenkamp reported FY2024 projects are underway and will change how SERS provides service. Ms. Roggenkamp mentioned the meeting would include an update on where SERS is headed in terms of shaping strategy and policy around Artificial Intelligence (AI).	

Technology Roadmap – Progress Update: MVVM Upgrade

Jay Patel, SERS Chief Technology Officer, shared an update on FY2024 SMART projects, beginning with the Reimagine MSS Portal Registration project. The project kicked-off on August 15 and deployment is planned for late Q2 FY2024. Next, Mr. Patel provided an update on the now deployed MVVM Upgrade which makes MSS and eSERS portals now functional on cellphones and tablets. Mr. Patel reported this project deployed in production on August 4 and took significant effort across the organization and the result will be helpful for members. Mr. Patel reports there has been positive feedback from users and made a point to thank staff for their tremendous commitment to getting this project done. Mr. Patel went over statistics and metrics for the now deployed project and reports post-production support will be on-going.

Mr. Patel opened the floor to questions. Board member, Frank Weglarz inquired if many issues were found in 30-day warranty window for the MVVM project. Mr. Patel reported most issues found were related to clarification and any issues found were fixed.

Mr. Patel continued his report on the remaining FY24 SMART project timelines and estimated budgets. The Refund Reimagination project will allow members to have self service capability. An Agile project team has been formed to analyze current challenges and a kick-off meeting was held to initiate the discovery process. The eDelivery project will allow SERS to send communication to members effectively through email and texting. A Master Agreement and Statement of Work to upgrade Planet Press Software is under review as the current software is coming to an end of life. Finally, Mr. Patel reported the ePayments – Other System Transfer and ePayment – Employer and CSPC projects are on track and. Expected to deploy by December 2023 and on budget.

Mr. Patel continued with the FY24 infrastructure projects update. The Committee received a detailed timeline of all infrastructure FY24 projects and Mr. Patel provided an update that the phone system replacement RFP process is underway. The Network and wireless Refresh project was completed on September 08, 2023, and has been a major lift for IT by modernizing infrastructure in terms of the network. This project is expected to be under budget by approximately $70K. Mr. Patel concluded there is no breaking news on the remaining projects.

Next, Mr. Patel provided a status update on the Commvault cloud storage for back-up commitment. Mr. Patel reminded the committee that this matter was brought to the full Board in February 2022 as a request to move SERS backup data into the cloud and stop the daily outbound transfer of tapes to the offsite storage vendor (FireProof). Daily inbound transfer of tapes from FireProof to SERS continued so existing tapes can be recycled, and an update was provided in December 2022. Mr. Patel reported as of the end of FY2023, SERS received ~1,200 tapes from Fireproof and they have all been recycled. It has been one year since SERS has done any tape back-ups and reported it all goes to cloud storage.

Mr. Patel continued his presentation going over the Technology Roadmap Budget, reporting there are no significant updates. Mr. Patel reminded the Committee that FY24 will be an active year, and this is a fluid budget in that the money carries forward, and we are tracking to the budget we have allocated for FY2024.

The Committee thanked Mr. Patel for his presentation.

Information Security Update

Ms. Roggenkamp introduced the next topic of AI, reporting it is a quickly developing area that holds exciting possibilities in investments. Ms. Roggenkamp explained AI can be viewed in two ways, how does it benefit us and how do we utilize it in a very secure manner. Ms. Roggenkamp introduced SERS Chief Risk Officer, Joe Bell, to discuss further. Mr. Bell echoed the sentiment that AI is continually evolving, and SERS is looking at the risks and opportunities. Mr. Bell reported on a contract in place with Linea Solutions, a company of subject matter experts in AI and pensions systems, in an effort to ensure there is a good governance structure in place. This consultant will aid SERS with strategy, policy, tools/platforms, and security. Additionally, SERS will remain in touch with other pension systems that have implemented tools involving AI. SERS strategy is to use these resources to continue a path towards setting the right strategy and culture around AI. Mr. Bell concluded the AI discussion by noting nothing comes without risk, and SERS will put a plan in place with due consideration of those risks.

Mr. Bell, continued with the Information Security update, providing an update on planned communication to members and retirees on safeguards over their sensitive data. At the request of the Committee, Mr. Bell and his team will provide communication to SERS' members and retirees about what is being done to protect their data and be cognizant of the protected data of theirs that SERS is responsible for. At this time a draft plan is to include these updates in the quarterly retiree newsletter and website portal account login. Board member, Frank Weglarz suggested quicker movement on getting this information out to the members due to online petition signing which asks for members and retirees to give their last four digits of their social security number. Board member, Dan Wilson asked why the last four digits of a social security number are needed and recommended eliminating that request. Executive Director, Richard Stensrud, explained members and retirees are given an option to provide either the last four digits of their social security number or the last four digits of their SERS membership ID. Mr. Bell concluded on an assurance to involve the chair when the communication on safeguards over sensitive data is rolled out.

Mr. Bell continued his report by providing the key metrics on Information Security's three lines of defense: Proofpoint, Microsoft, and Staff. There were no incidents to note in this last quarter. SERS continues to inform staff on how to be more secure and have good cyber hygiene. When issues are recorded, Information Security works closely with IT to make sure those vulnerabilities do not have an impact. Mr. Bell once again reported that SERS' cyber exposure is slightly lower than industry average, however, planned replacement of aging infrastructure within the next year is expected to help address these vulnerabilities. Older equipment gives a higher risk score, but there is a remediation plan in place. Mr. Bell assured the Committee they will continue to see these metrics, but it is not new, different, or concerning.

Mr. Bell continued his report on inboard email and blocked messages. This data comes from Proofpoint, SERS' front-end filter. This tool helps to look at this and roughly takes out between 66% - 70% of threats. Mr. Bell went over typical threats such as sender intelligence, phishing attempts, spam, and malware. AI looks at the type of inbox emails coming in and if it recognizes a threat, it knocks them out before they get any further. Once the email goes through Proofpoint it then goes through Microsoft which looks for further anomalies. Mr. Wilson inquired if there are any standards of organizations our size to compare to see if this is normal activity in terms of volume. Mr. Bell confirmed he will investigate this matter, but reports it is likely consistent with the volumes SERS experiences.

	The Committee thanked Mr. Bell for his presentation. **Executive Session** Frank Weglarz moved, and James Rossler seconded the motion that the Technology Committee convene in Executive Session pursuant to R.C. 121.22(G)(6) to discuss security matters. Upon roll call, the vote was as follows: Yea: Matthew King, James Rossler, Frank Weglarz, Daniel Wilson. The motion carried. The committee convened in Executive Session at 1:32 p.m. The committee returned to open session at 1:47 p.m. **Upcoming Technology Committee Meetings – Future Topics and Next Meeting Dates** Board member, Dan Wilson, asked if SERS waits for a new technology roadmap budget or if it is viewed as a rolling five years. Ms. Roggenkamp explained we look at the $8.3 million as a rolling budget. A rolling budget adds a future period's budget to replace a budget for a period that has passed. With the always evolving changes in Technology, SERS IT projects will be completed, and new projects will be added to keep our technology current. The Technology Committee and Staff will refresh the rolling budget at the end of each fiscal year as part of the annual budget process. The next regular Technology Committee meeting will be held Thursday, December 21, 2023, at 12:30 pm or immediately following the regular SERS Board Meeting. Technology Committee Chair, Matthew King, adjourned the meeting at 1:49 p.m.		
	Action Items	**Assigned Person**	**Due Date**
Action Items	n/a		

TECHNOLOGY COMMITTEE

December 21, 2023

Agenda

- **Opening Remarks** (Matt)
- **Executive Session for Security Matter** (SERS Staff)
- **Artificial Intelligence (AI) and SERS** (Karen, Joe, Jay)
- **Information Technology Update** (Jay)
  - Infrastructure
  - SMART
- **Risk Management and Information Security – Update** (Joe)
  - Quarterly Information Security Metrics
- **Future Topics** (Committee and Staff)

EXECUTIVE SESSION

_____ moved and_____seconded the motion that the Technology Committee convene in Executive Session pursuant to R.C. 121.22(G)(6) to discuss a security matter.

Upon roll call, the vote was as follows:

ROLL CALL:	**YEA**	**NAY**	**ABSTAIN**
James Rossler	_____	_____	_____
Frank Weglarz	_____	_____	_____
Daniel Wilson	_____	_____	_____
Matthew King	_____	_____	_____

IN EXECUTIVE SESSION AT _____ A.M./P.M.

RETURN TO OPEN SESSION AT_____A.M. / P.M.

Types of AI Technologies

"Artificial intelligence is as revolutionary as mobile phones and the Internet." – Bill Gates

What is AI? A machine's ability to perform cognitive functions we usually associate with the human mind.

Generative AI

Generates content in response to a prompt

Machine Learning

Algorithms trained on data to detect patterns and learn how to make predictions and recommendations

Deep Learning

Machine learning that processes a wider range of data resources (images, in addition to text)

SOURCE: McKinsey & Company (excerpts)

SERS will implement an AI Culture that balances risks and opportunities from AI technologies.

Pension System Risks and Opportunities

AI Risks
1. **Security Concerns:** AI systems can be vulnerable to cyber attacks, putting sensitive pension data at risk. Ensuring robust cybersecurity measures is crucial.
2. **Bias and Fairness:** If the AI algorithms used in the pension system are biased, it could result in unfair treatment, impacting certain demographic groups negatively.
3. **Lack of Human Oversight:** Overreliance on AI without proper human oversight may lead to errors or decisions that lack empathy and understanding of unique individual circumstances.

SOURCE: ChatGPT

Pension System Risks and Opportunities

AI Opportunities
1. **Efficiency and Automation:** AI can streamline processes, reduce manual workload, and enhance overall efficiency in managing pension-related tasks and transactions.
2. **Personalized Planning:** AI algorithms can analyze individual financial situations by offering a tailored approach, optimizing choices, and ensuring better retirement outcomes.
3. **Fraud Detection:** AI can play a vital role in detecting and preventing fraudulent activities, ensuring the integrity of the pension system.
4. **Data Analysis for Better Investments:** AI can analyze vast amounts of financial data in real-time, helping pension funds make more informed investment decisions and potentially increasing returns.
5. **Improved Customer Service:** Chatbots and virtual assistants powered by AI can provide instant, 24/7 customer support, addressing queries and concerns efficiently. They can also assist in problem escalation.

SOURCE: ChatGPT

SERS Governance

1. AI Oversight Committee – Strategic Planning Committee subset, Approve AI Uses
2. Culture/Organization Change Mgmt – Communication and Training Plans for Staff
3. Board Awareness – Training (Linea)
4. Policy Development – Guidance, Responsible / Prohibited Uses
5. Intake Form – Risk and Opportunity; Communicate AI Tool Needs = No Rogue
6. Vendor Management – Onboard Controls, Align NIST-AI Standards
7. Monitoring – IT, Security, Internal Audit, External Reviewers
8. Expert Advisors – Linea
9. Capability Maturity – Best Practice Alignment, Continuous Improve (Linea)

Responsible AI Uses

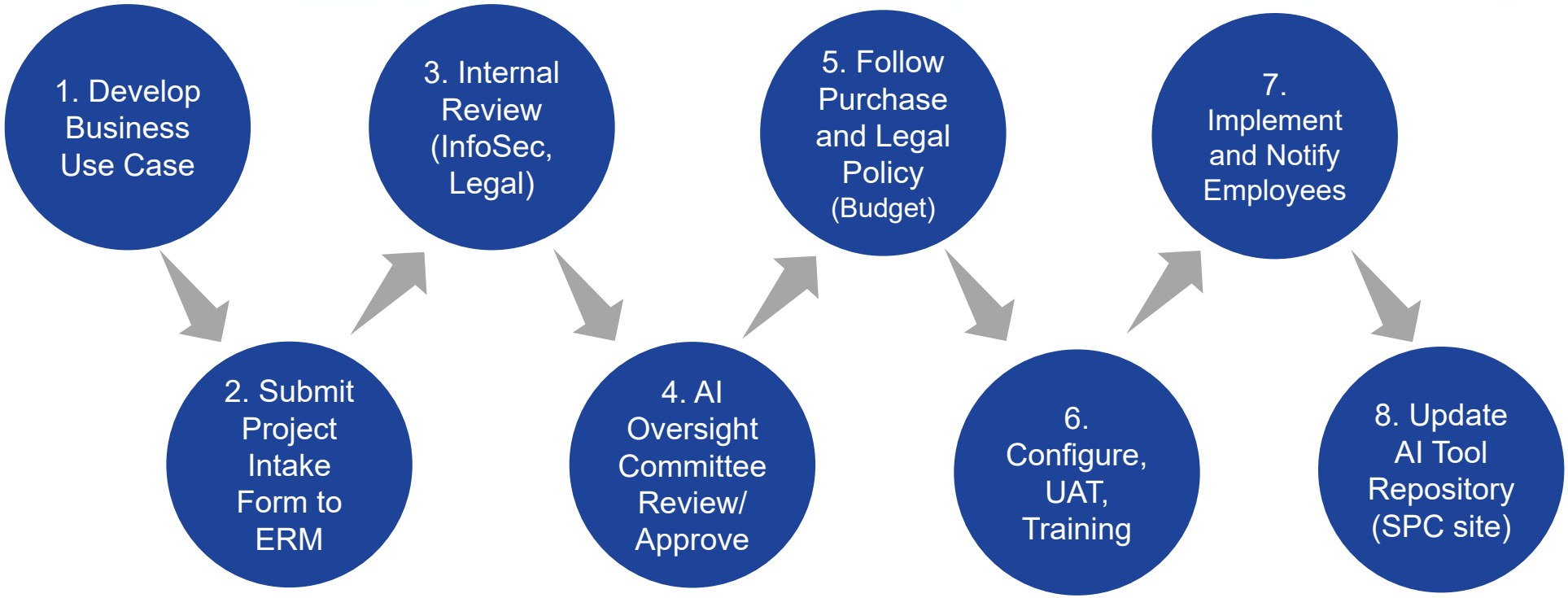
1. Virtual assistants or chatbots to support customer service
2. Brainstorm ideas for a project or research topic
3. Create software tool efficiencies
4. Develop, debug, or test software code
5. Generate draft communication
6. Statistical data analysis and predictive modeling
7. Security and fraud-preventive controls
8. Other uses, as approved by SERS' AI Oversight Committee

All AI–generated output must be verified by employee for accuracy. Questions about appropriate use of AI resources can be directed to the employee's supervisor, IT, Legal, or Risk Management.

Prohibited AI Uses

1. Conduct illegal, unethical, or malicious activities (hack, fraud, harassment, unauthorized access).
2. Threaten digital security of individuals or systems through social engineering or deepfakes.
3. Discriminate against individuals based on age, race, color, religion, sex, gender identity, military status, familial status, national origin, sexual orientation, disability, genetic information, or any other factor protected by law.
4. Submit member data (PII, PHI) or sensitive/proprietary data into a shared AI platform (info can become public in a LLM – Large Language Model).
5. Disseminate misleading information with the intent to deceive or manipulate others.
6. Invade privacy, conduct surveillance, or use personal information without consent.
7. Present AI-generated content as the work of a human when interacting with others, unless explicitly disclosed as AI-generated.
8. Use SERS-provided AI technologies for personal use.

Internal Approval Process



Potential AI Use Cases

1. Generative AI Tools
   - ChatGPT / Claude (chat interface)
   - Bing Enterprise (chat interface, verify data source)
   - M/S 365 Copilot (chat interface)
   - Meeting Recap (Zoom, Fathom, M/S Intelligent Recap – GCC Tenant)
   - Custom Chatbots (Heavy Data Sources - CalSTRS; SMART)
   - Website Chatbot (User Activity Analysis)
2. Contact Center (CCaaS Communications, Observe AI – Missouri PSRS)
3. Software Development/Review/Refactoring (GitHub Copilot - Missouri PSRS)
4. Identity Verification/Proofing/Fraud (MSS Portal - Socure, OPERS/DAS)
5. Investments (Machine Learning Algorithms - Predictive Analytics, TxTRS)
6. Cybersecurity Tools (Arctic Wolf security monitoring, Proofpoint email)

CHALLENGES: Tool Available, Minimum # Licenses, Technology Fit, Cost/Budget, Vendor/Tool Stability, Need Priority

Expectations for Leadership

1. Become knowledgeable about AI's opportunities and challenges
2. Embrace change it will bring – provide leadership and accountability
3. Provide reinforcement and ongoing support for staff, especially those that may struggle with the AI change journey
4. Work closely with ERM to mitigate organizational risks
5. Ensure AI policy is well understood and complied by staff
6. Be patient as AI Oversight Committee assesses risks and priorities

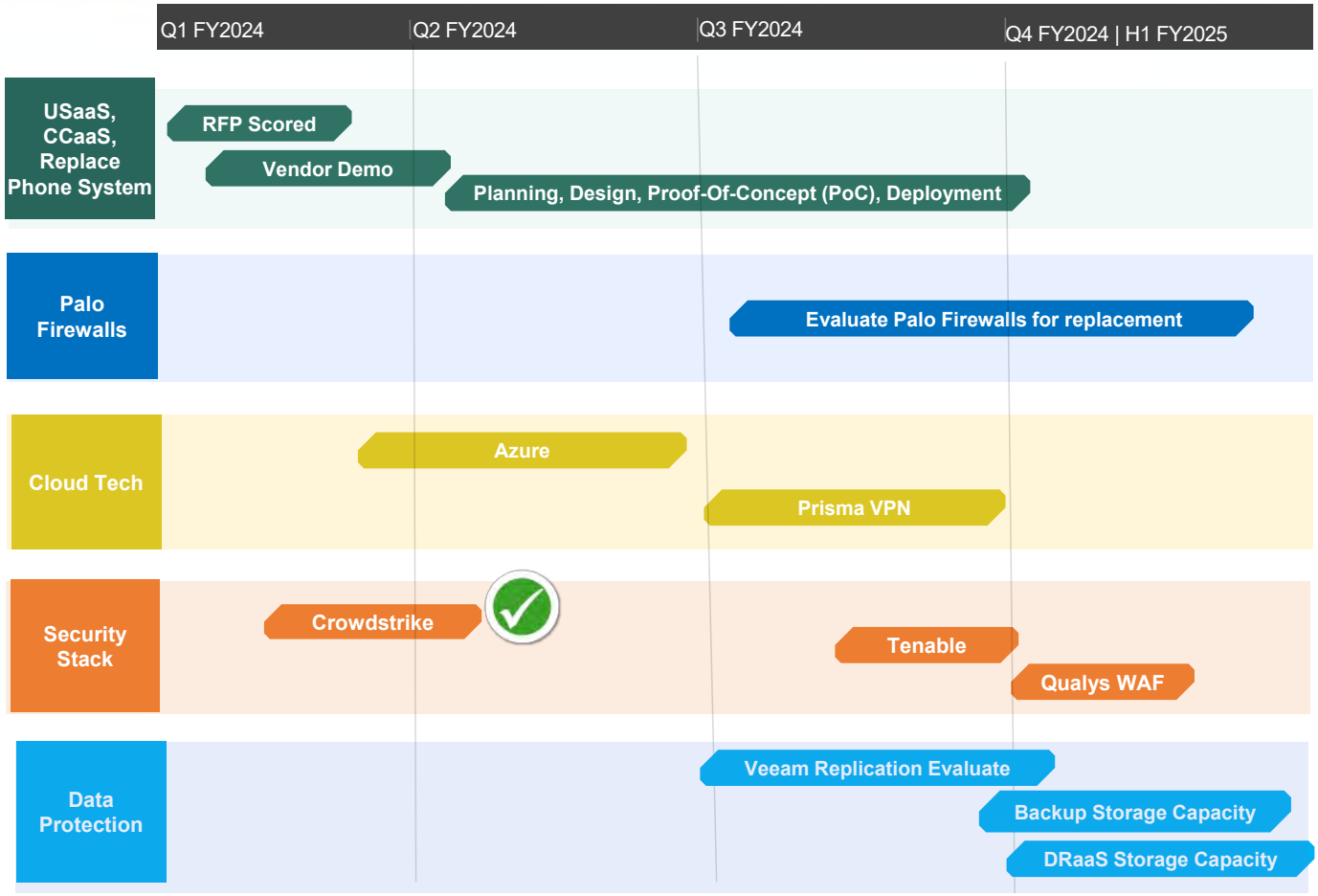
Guess What? Now Every Vendor is an AI Vendor

SELECTION

INFORMATION TECHNOLOGY UPDATE

Technology Roadmap

Technology Roadmap – FY2024 Infrastructure Projects



- RFP response review and demo complete.
- 3 vendors were selected for additional PoC.
- Vendor has been selected and going through MSA with an anticipated project start date in Jan 2024.

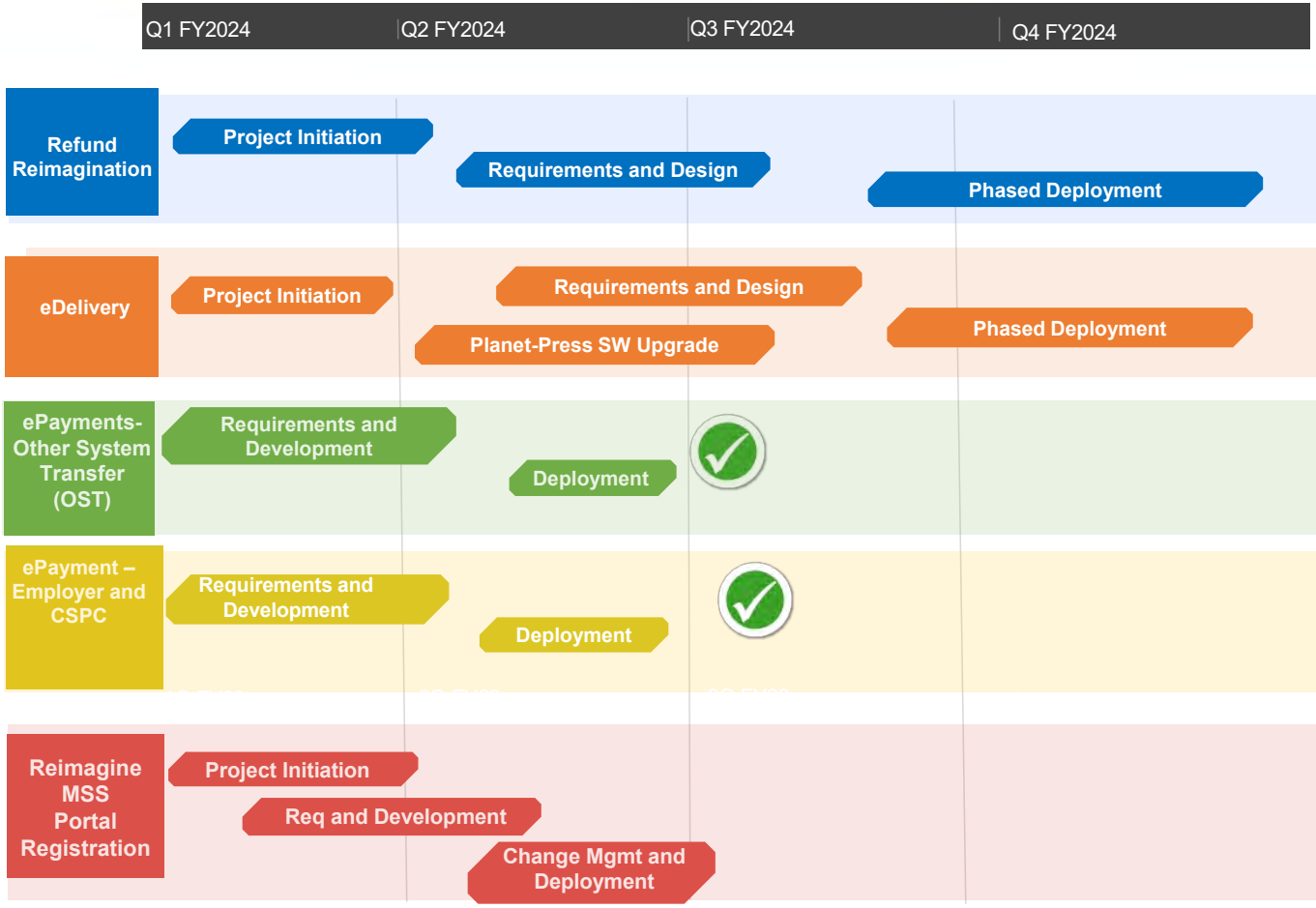
- Two physical Palo Alto Firewalls purchased May 2021
- SERS network hardware recently upgraded
- Best practice: every 3-5 years evaluate for replacement

- Azure Virtual Desktop proof of concept
- Azure SQL Platform as a Service exploration and analysis
- Cloud-based VPN increasing resiliency.

- IT and IS evaluated Crowdstrike for end-point protection and retained.
- Tenable expires May 2024
- Qualys WAF expires June 2024

- Veam Replication Evaluation ($40,000)
- Expand Backup storage capacity ($52,500)
- DRaaS Storage capacity ($25,000)

Technology Roadmap – FY2024 SMART Projects



- Team continued to study current refund process and identify requirements for improvements.
- Analysis, design and development iteration is in progress.

- MSA and SOW to upgrade PlantPress Software was completed.
- Agile project team was formed, and project has kicked off.

- Project team has been formed and requirements analysis and design is underway.
- Project was deployed in production ahead of schedule and on budget ($20,312).

- Project team has been formed and requirement analysis and design is underway.
- Project was deployed in production ahead of schedule and on budget ($28,295).

- Development was completed.
- Member and Employer change management activities were initiated.
- Testing including end-user experience and operational support process is in progress.

Technology Roadmap – Budget

Five Year Technology Roadmap Budget						
Description	Total 5-Year Plan	FY2023 Actual Spend	FY2024 Plan*	FY2024 Spend to Date	Total Roadmap Spend to Date	Remaining Roadmap Amount **
Telecommunications	$ 250,000	$ 175,848	$ 206,491	$ -	$ 175,848	$ (132,339)
Security Stack	$ 899,600	$ -	$ 432,200	$ 24,790	$ 24,790	$ 467,400
Network Infrastructure Refresh	$ 886,000	$ 638,914	$ 120,000	$ 13,338	$ 652,252	$ 127,086
Hybrid Technology Replacement	$ 419,000	$ 121,297	$ 10,000	$ -	$ 121,297	$ 287,703
Server Infrastructure	$ 1,216,700	$ -	$ 288,100	$ -	$ -	$ 928,600
Backup and Recovery	$ 532,754	$ 140,455	$ 117,500	$ -	$ 140,455	$ 274,799
SMART Portals	$ 196,000	$ -	$ 196,000	$ 26,250	$ 26,250	$ -
SMART Framework	$ 760,000	$ 175,000	$ 510,000	$ 175,000	$ 350,000	$ 75,000
SMART Enhancements	$ 2,623,000	$ 73,836	$ 855,000	$ 21,250	$ 95,085	$ 1,694,165
SMART Business Tools	$ 500,000	$ 96,400	$ 250,000	$ 108,896	$ 205,296	$ 153,600
SMART total	$ 4,079,000	$ 345,236	$ 1,811,000	$ 331,395	$ 676,631	$ 1,922,765
Infrastructure Total	$ 4,204,054	$ 1,076,514	$ 1,174,291	$ 38,128	$ 1,114,641	$ 4,165,926
Total Budget	$ 8,283,054	$ 1,421,749	$ 2,985,291	$ 369,523	$ 1,791,272	$ 3,876,014

* Two infrastructure projects have been realigned with category descriptions to better reflect their underlying expense.

The total FY2024 Plan did not change.

** Remaining Roadmap is equal the Total 5-Year Plan less FY2023 Actuals and less FY2024 Plan

RISK MANAGEMENT AND INFORMATION SECURITY UPDATE

Quarterly Update

Artificial Intelligence (AI)

- AI Policy (hard copy) - will continue to evolve
- Weekly and intermittent governance and implementation process with AI consultant (Linea); future focus on risk review and tool considerations

External Penetration Test – Member and Employer Self Service Portals

- Positive results – no critical or high comments; developing remediation plan

Bi-Annual Tabletop Exercise – Cyber Scenario (Kroll – Jan. 17th)

Communication on Protecting Member Data

- *Retiree Focus* newsletter (January)
- Member portal Account Login screen - new Data and Security Section (December)

Quarterly Metrics

- Key measure benchmarks and third-party security monitoring did not identify any security incidents in last three months

Quarterly Information Security Metrics

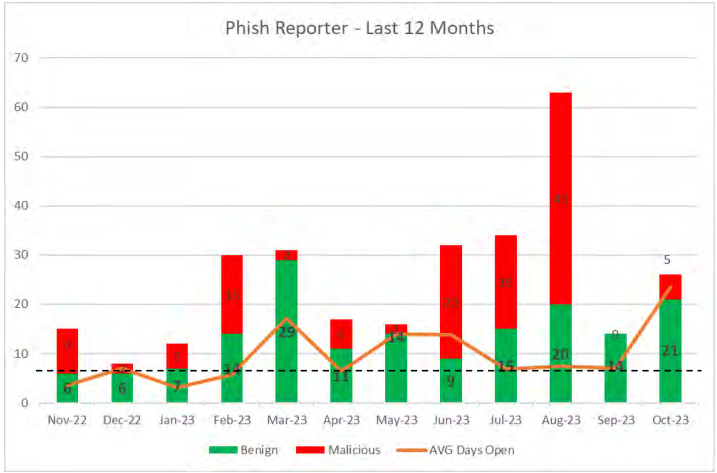
September - December 2023

Information Security – Key Metrics

Security Awareness Training > 90% Goal - MET

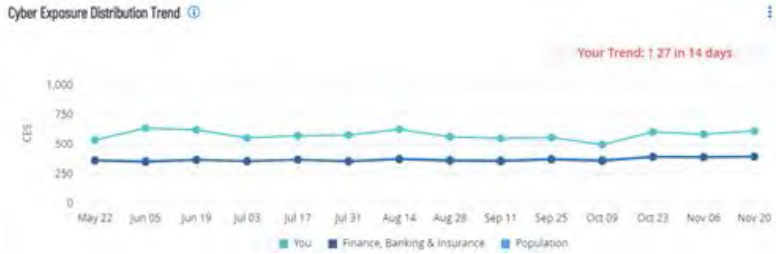
Three Lines of Defense:

1. Proofpoint
2. Microsoft
3. Staff



Phish Reporting & Response < 7-day goal – PARTIALLY MET
(NOTE: Process Change/Improve Response to Hours - November)

Maturity > Peer Benchmarks - MET
(Addressing Vulnerabilities)

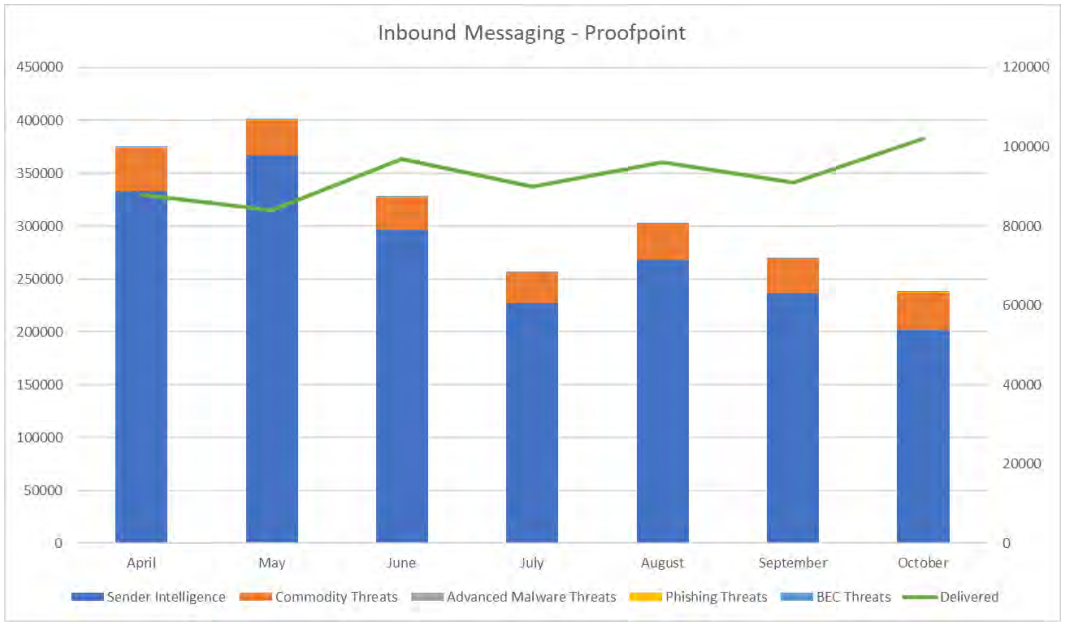


Cyber Exposure < Peer Benchmarks – NOT MET
(Average Asset Exposure Score - Vulnerability Remediation Plan)

Metrics: Inbound Email and Blocked Messages

Proofpoint Highlights Include:

- Inbound emails: 240,000 – 400,000 / month
- Emails delivered: 85,000 – 95,000 / month



Typical threats:

- ❖ Sender Intelligence (reputation)
- ❖ Commodity (spam, malware)
- ❖ Advanced Malware (targeted attack)
- ❖ Phishing (steal credentials)
- ❖ BEC (business email compromise)

Peer Metrics: Currently unavailable, however, SERS risk profile index higher due to size (AUM), available public info (website, records, Ohio Checkbook), threat actors' reputation, and number/severity of threats.

QUESTIONS

Future Topics

ADJOURNMENT(R)

_____ moved that the Technology Committee adjourn to meet on _____ for the next scheduled meeting.

The meeting adjourned at _____ p.m.

_____
Matthew King, Chair

Artificial Intelligence (AI) Usage Policy

EX7-003

Effective Date:	11/29/2023	**Revision Date:**	11/29/2023	**Audience:**	Everyone
Owner:	Executive	**Certifier:**	Richard Stensrud	**Co-Owners:**	Information Technology
Document Links:	Purpose, Policy, Procedure, Definitions, Related Documents, Policy History				

Purpose

To establish guidelines, and best practices on SERS' use of Artificial Intelligence (AI) technologies and tools. This policy is intended to enable our technical, business, and legal decision-makers to leverage AI while protecting our data, values, and mitigating risks.

Policy

SERS is committed to using AI technologies in an ethical and responsible manner, and adhering to applicable laws, regulations, and industry standards. We will ensure AI systems are used with transparency, explainability, accountability, and fairness in mind, avoiding any use that may result in harm, discrimination, or infringement on individuals' rights and privacy. We remain committed to adopting new technologies to aid our mission and will balance the risks and limitations of AI to ensure its responsible use.

Governance

SERS' Strategic Planning Council (SPC) and Risk Management staff are responsible for providing guidance, interpretation, and direction of AI implementation. A subset of the SPC will review and approve AI tools to ensure alignment with SERS' mission, objectives, security requirements, technical fit, and operational direction.

SERS' AI Oversight Committee shall consist of:

- Executive Director/Deputy Executive Director
- General Counsel
- Chief Risk Officer
- Chief Technology Officer
- Chief Financial Officer
- Assistant Director, Engagement & Communications
- Other Subject Matter Experts, as needed

Compliance, Standards and Practices

AI is in a state of rapid evolution and adoption with limited legal and regulatory requirements. SERS will establish and maintain the appropriate accountability mechanisms, roles and responsibilities, culture, and structures for risk management to be effective. SERS will tailor its practices to incorporate elements from the U.S. National Institute of Standards and Technology's (NIST) AI Risk Management Framework.

The Framework's underlying premise is to create dialogue, understanding, and responsible risk management that results in trustworthy AI systems. Characteristics of trustworthy AI systems include: valid and reliable, safe, secure and resilient, accountable and transparent, privacy-enhanced, explainable and interpretable, and fair with harmful bias managed. The Framework also provides four core functions used to manage AI risks for the development of trustworthy AI. They include:

1. Govern: Culture of Risk Management
2. Map: Identify Risks
3. Measure: Evaluate Risks
4. Manage: Prioritize High Impact Risks

The ethical use of AI by SERS' employees is essential to developing trustworthy AI systems. SERS will incorporate values-based principles (e.g. human-centered values and fairness) identified in the Organization for Economic Co-operation and Development (OECD) Principles on AI.

Once implemented, management will implement controls to ensure proper reliance can be placed on the AI-generated output. Periodic monitoring may include reviews by risk management, information security, internal audit, and external reviewers.

Records of AI outputs may be subject to open-records requests and must be maintained in accordance with SERS' Records Retention Schedule. The AI Oversight Committee will work with ERM to determine how AI outputs are documented and identified.

Use of AI technology must comply with all applicable information privacy and security laws and regulations and all SERS policies and procedures, including without limitation, SERS' Ethics Policy; Standards of Professional and Ethical Conduct for Employees; HIPAA Information Security; Information Security; Access to Business Systems and Data; Appropriate use of Computers and Related Technologies Systems Policy; Cloud Policy, Data Management Policy; Vendor Risk Management; Use of Communication Systems; Communications Policy; and Records Retention Program Guidelines.

AI Usage

If use of AI technology is approved, SERS' employees will be required to complete training and demonstrate proficiency in the proper use of the specific approved AI technology as determined by the AI Oversight Committee. Training on AI technology generally must be performed in a non-production environment prior to implementation in a production environment.

Employees are authorized to use only approved AI technologies.

Output generated by AI technologies must be verified by an employee for accuracy. If a reliable source cannot be found to verify information generated by AI, that information cannot be used for work purposes.

Responsible AI uses may include:

- Virtual assistants or chatbots to support customer service
- Brainstorm ideas for a project or research topic
- Create software tool efficiencies
- Develop, debug, refactor, or test software code
- Generate draft communication
- Statistical data analysis and predictive modeling
- Security and fraud-preventive controls
- Other uses, as approved by SERS' AI Oversight Committee

Staff are prohibited from using member data (PII, PHI) or sensitive/proprietary data in a shared AI platform. Information can become public in a Large Language Model (LLM).

Additionally, staff are prohibited from using AI to:

- Conduct illegal, unethical, or malicious activities (hacking, fraud, harassment, unauthorized access)
- Threaten digital security of individuals or systems through social engineering or deepfakes
- Discriminate against individuals based on age, race, color, religion, sex, gender identity, military status, familial status, national origin, sexual orientation, disability, genetic information, or any other factor protected by law
- Disseminate misleading information with the intent to deceive or manipulate others
- Invade privacy, conduct surveillance without authorization, or use personal information without consent
- Present AI-generated content as the work of a human when interacting with others, unless explicitly disclosed as AI-generated
- Use SERS-provided AI technologies for personal use

Use of AI may result in unauthorized use or disclosure of others' confidential information or intellectual property and violate copyright, trademark, trade secret, patent, or other intellectual property laws. Employees may not use AI technology to replicate or modify existing intellectual property without the express written permission of the intellectual property owner.

SERS will continue to provide training, guidance, and ongoing support to staff on all AI matters to help them gain better understanding, familiarity, and use of AI tools to enhance their job function. Employees should report any issues or concerns related to the use of AI technology and any potential violations of this policy to their supervisor or IT. A service ticket should be created immediately to track and resolve any potential

violations. Questions about appropriate use of AI resources can be directed to the employee's supervisor, IT, Legal, or Risk Management.

Violations of this policy are subject to corrective action, up to and including termination of employment.

Procedures

Requesting an AI Use Case Review

Requesting an AI Use Case Review

The internal review and approval process for AI tools will typically occur as follows:

1. Process Owner develops an AI business use case for their Department Director's consideration.
2. SERS' Director/designated staff submit AI Project Intake Form request to ERM Officer to evaluate overall risks involving the AI tool.
3. ERM completes risk assessment that includes an evaluation of Information Security and Legal risks.
4. AI Oversight Committee will review and approve the AI tool's intended use, opportunity, risks, security and compliance concerns, technical fit, budget implications, and implementation plan. Unapproved use cases may be resubmitted once additional information is obtained; however, AI tools may not be used without approval of the AI Oversight Committee.
5. Once approved, the Process Owner will follow procurement and legal requirements.
6. Process Owner will collaborate with IT for the implementation of the AI tool. This includes, but is not limited to deployment and configuration, user acceptance testing, training for users, and future support and maintenance.
7. Upon implementation, affected employees will request or be notified by IT of their access rights.
8. An inventory of approved AI technologies will be maintained on the SPC's SharePoint Site.

Definitions

Artificial Intelligence (AI) - applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions.

Deepfake - video of a person in which their face or body has been digitally altered so they appear to be someone else, typically used maliciously or to spread false information.

Explainability - easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

Related Documents and Information

Statutes:	National AI Initiative Act of 2020, NIST AI Risk Management Framework (AI RMF 1.0, January 2023), NIST Trustworthy and Responsible AI Resource Center (AIRC, March 2023), Organization for Economic Co-operation and Development (OECD) Principles on AI
Rules:	N/A
Document Links:	Purpose, Policy, Procedure, Definitions, Related Documents, Policy History
Forms:	---

Policy History

None