NEW JERSEY CYBER RISK MANAGEMENT FUND

MEETING AGENDA
Thursday, June 18, 2026 – 1:30PM
Via Zoom Audio/Video

Please choose 1 Option to join:

1. **Zoom Link: https://permainc.zoom.us/j/97482447647**
2. **Dial-In: 309 205 3325 Meeting ID: 974 8244 7647#**
3. **One tap mobile: +13092053325,,974 8244 7647#**

STATEMENT OF COMPLIANCE WITH OPEN PUBLIC MEETINGS ACT

The NJ Cyber Risk Management Fund will conduct this meeting in accordance with the Open Public Meetings Act, N.J.S.A. 10:4-6 et seq. Notice of this meeting was given by (1) sending sufficient notice herewith to the Star Ledger and Courier Post; (2) sending notice of this meeting with member joint insurance funds and (3) posting this notice on the public bulletin board of all members.

NEW JERSEY CYBER RISK MANAGEMENT FUND
Thursday June 18, 2026 – 1:30PM
Via Zoom Audio/Video

- ❑ **Meeting Called to Order – Open Public Notice to be Read**
- ❑ **Pledge of Allegiance**
- ❑ **Roll Call of Fund Commissioners**
- ❑ **May 21, 2026 Open Minutes.....Appendix I**
- ❑ **Correspondence**: None

REPORTS

- ❑ **AUDITOR**
  Financial Audit Report & Management Report as of December 31, 2025 .....**Separate Attachment**

- ❑ **ACTUARY – The Actuarial Advantage**
  Valuation Report as of December 31, 2025 .....**Separate Attachment**

- ❑ **Executive Director**
  Report .....Page 1
  Resolution 32-26 to Certify Audit Report .....Page 3

- ❑ **Treasurer**
  June 2026 Bills List – Resolution 33-26 .....Page 23

  MOTION TO ADOPT RESOLUTION 33-26 APPROVING THE JUNE 2026 VOUCHER LIST AS SUBMITTED

- ❑ **Underwriting Manager**
  Report .....Verbal

- ❑ **Attorney**
  Report .....Verbal

- ❑ **Old Business**

- ❑ **New Business**

- ❑ **Public Comment**

- ❑ **Executive Session – For Certain Specified Purposes - Personnel -Safety & Property Of Public – Litigation**

Next Meeting is scheduled for July 16, 2026 at 1:30 PM via Zoom

- ❑ **Adjournment**

NEW JERSEY CYBER RISK MANAGEMENT FUND
9 Campus Drive – Suite 216
Parsippany, NJ 07054
Tel 201.881.7632

Date: Thursday, June 18, 2026

To: Board of Fund Commissioners
New Jersey Cyber Risk Management Fund

From: Perma Risk Management Services

- **Audit Report and Actuary Valuation Report as of December 31, 2025:** The Audit Report as of December 31, 2025 is enclosed separately. A representative from Nisivoccia will be present at the meeting to review the report. Also enclosed separately is the Actuary's Year End Valuation Report. Resolution 32-26 Certifying the Audit Report and the Group Affidavit, indicating that each member of the Board has read the General Comments Section of the Audit Report, is included on **pages 3-6**.
  - **Motion to Approve Year-End Financials, Adopt Resolution No. 32-26 and execute Group Affidavit indicating that the Fund Commissioners have read the General Comments Section of the Audit Report.**

- **Operations Committee:** The Committee met virtually on June 18th at 11:15 a.m.; the Committee discussed the following:
  - **Risk Control Services:** Ad Hoc committee has met twice and consulted with the Chertoff Group and member IT personnel to develop modifications to the scope of services for cyber training/phishing simulation and vulnerability external scanning. Operations Committee met and reviewed the proposed changes submitted to the Underwriting Manager. Included on **pages 7-17** are the proposed changes, which are outlined in red.

  - **Zero Trust Deployment**: The Chertoff Group prepared the attached Zero Trust Guide material for members to utilize. Operations Committee reviewed the material. The Underwriting prepared a companion worksheet in excel to complement the Chertoff Group's work. The attachments are provided separately.

- **Claims Committee:** There were no PARs since our last meeting in May. A Claims Detail Report as of 5.30.2026 was sent to the Fund Commissioners under separate cover.

- **Cyber JIF Website:**
  - **Website Updates:** Fund Office is in the process of updating the website to include the amended 3rd party risk assessment tool, revised cyber framework with the amended deductible incentive structure and the two bulletins on cyber risk alerts.

  - **Website Usage:** Princeton Strategic Communications also reported at the MEL Safety and Education Committee on, among other topics, statistics on the Cyber JIF website usage. Information from their report pertaining to the Cyber JIF website is on **page 18** of the agenda.

- **Cyber Educational Series:** Underwriting Manager is scheduled to hold the 1st webinar of the educational series on June 23rd at 10 a.m.. The notice that included the link to register was distributed to membership on June 15th and is also included on **page 19**.

- **Due Diligence:**
  - Financial Fast Track – For information attached is another copy of the 1st quarter report. (**page 20**)
  - Loss Ratio Report as of May 31, 2026 (**page 22**)

- **Next meeting**: The next Cyber JIF meeting is scheduled for July 16, 2026 at 1:30 PM via audio / video teleconference.

Resolution No. 32-26

Resolution of Certification
Annual Audit Report for Period Ending December 31, 2025

WHEREAS, N.J.S.A. 40A:5-4 requires the governing body of every local unit to have made an annual audit of its books, accounts and financial transactions, and

WHEREAS, the Annual Report of Audit for the year 2025 has been filed by the appointed Fund Auditor with the Secretary of the Fund as per the requirements of N.J.S.A. 40A:5-6 and N.J.S.A. 40A:10-36, and a copy has been received by each member of the Executive Committee, and

WHEREAS, the Local Finance Board of the State of New Jersey is authorized to prescribe reports pertaining to the local fiscal affairs, as per R.S. 52:27BB-34, and

WHEREAS, the Local Finance Board has promulgated a regulation requiring that the Executive Committee of the Fund shall, by resolution, certify to the Local Finance Board of the State of New Jersey that all members of the Executive Committee have reviewed, as a minimum, the sections of the annual audit entitled:

General Comments
and
Recommendations

and

WHEREAS, the members of the Executive Committee have personally reviewed, as a minimum, the Annual Report of Audit, and specifically the sections of the Annual Audit entitled:

General Comments
and
Recommendations

as evidenced by the group affidavit form of the Executive Committee.

WHEREAS, such resolution of certification shall be adopted by the Executive Committee no later than forty-five days after the receipt of the annual audit, as per the regulations of the Local Finance Board, and

WHEREAS, all members of the Executive Committee have received and have familiarized themselves with, at least, the minimum requirements of the Local Finance Board of the State of New Jersey, as stated aforesaid and have subscribed to the affidavit, as provided by the Local Finance Board, and

WHEREAS, failure to comply with the promulgations of the Local Finance Board of the State of New Jersey may subject the members of the Executive Committee to the penalty provisions of R.S. 52:27BB-52 - to wit:

> R.S. 52:27BB-52 - "A local officer or member of a local governing body who, after a date fixed for compliance, fails or refuses to obey an

order of the director (Director of Local Government Services), under the provisions of this Article, shall be guilty of a misdemeanor and, upon conviction, may be fined not more than one thousand dollars ($1,000.00) or imprisoned for not more than one year, or both, in addition shall forfeit his office."

NOW, THEREFORE, BE IT RESOLVED, that the Executive Committee of the New Jersey Cyber Risk Management Fund, hereby states that it has complied with the promulgation of the Local Finance Board of the State of New Jersey, dated July 30, 1968, and does hereby submit a certified copy of this resolution and the required affidavit to said Board to show evidence of said compliance.

I HEREBY CERTIFY THAT THIS IS A TRUE COPY OF THE RESOLUTION PASSED AT THE MEETING HELD ON JUNE 18, 2026.

_____

Adam Brewer, Fund Secretary

GROUP AFFIDAVIT FORM
CERTIFICATION OF EXECUTIVE COMMITTEE
of the
NEW JERSEY CYBER RISK MANAGEMENT FUND

We members of the Executive Committee of the New Jersey Cyber Risk Management Fund, of full age, being duly sworn according to law, upon our oath depose and say:

1.) We are duly elected members of the Executive Committee of the New Jersey Cyber Risk Management Fund.

2.) In the performance of our duties, and pursuant to the Local Finance Board Regulation, we have familiarized ourselves with the contents of the Annual Fund Audit filed with the Secretary of the Fund pursuant to N.J.S.A. 40A:5-6 and N.J.S.A. 40A:10-36 for the year 2025.

3.) We certify that we have personally reviewed and are familiar with, as a minimum, the sections of the Annual Report of Audit entitled:

GENERAL COMMENTS – RECOMMENDATIONS

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

_____

(L.S.)

Attest:

_____

Adam Brewer, Secretary to the Fund

The Secretary of the Fund shall set forth the reason for the absence of signature of any members of the Executive Committee.

Important: This certificate must be sent to the Division of Local Government Services, CN 803, Trenton, NJ 08625

CYBER PHISHING AND TRAINING VENDOR

CC# 26-01

July XX, 2026, at 2:00 P.M.

New Jersey Cyber Risk Management Fund
9 Campus Drive, Suite 216
Parsippany, NJ 07054

CYBER SERVICES

CYBER TRAINING VENDOR
CYBER PHISHING VENDOR

I. SCOPE OF SERVICES

1. Security Awareness Training

a. The successful RESPONDER will provide access to online training for up to 38,000 employees of the FUNDs members – located throughout the state of New Jersey. At a minimum, the training program will include courses to cover the following topics:

Web Browsing How to navigate the internet and social media safely.	**Phishing & Email Security** How to identify common email scams and how phishing emails work.
Ransomware Learn to identify and prevent different forms of ransomware.	**Impersonation & Identity Theft** How to identify impersonation scams and protect your identity online.
Mobile Security Learn different vulnerabilities and protective measures when using mobile devices.	**Public Wi-Fi & Network Security** Lean what precautions you should take when connected to public Wi-Fi.
Insider Threat Learn what insider threat is, and how you can protect your place of work.	**Passwords** Learn how to create strong and effective passwords. Learn how your passwords can be modified for use on a variety of accounts.
Data Security & Encryption Learn the different types of data classification and how to properly protect them. Learn what data encryption is and how transmit data over email securely.	**Banking Exposures** Learn about the different types of banking exposures such as social engineering, reverse social engineering, funds transfer fraud.
Primer on Incident Response Learn about spear phishing, vishing, quishing, MFA fatigue/push bombing.	**Artificial Intelligence** Learn the proper use of AI (LLMS) in the workplace.

In addition, training in other areas of technology risk should also be available to be assigned to member employees by the member, the FUNDs Administrator, or the successful RESPONDER.

b. The training system should also include access to any other learning tools or resources that might be required for employees to experience the full benefit of the training session, or the responder shall provide for an educational system that will interact directly with the end user.

c. The training system shall provide a cloud-based learning management system that has customizable statistical data reports and metrics including progression, completion, and success rate by individual person, municipality, and each Joint Insurance Fund as a whole. The ideal training system should also have the capability to distribute reports automatically on a pre-determined schedule. The training system should be scalable to support all users across participating entities.

d. The ideal training system will be built on a platform that requires little to no administration by the FUND Administrator (other than as noted above). The system should be "turnkey" and fully managed by the successful RESPONDER, and directly coordinated with Entity's contact or their designee.

e. The training system shall be able to integrate with Microsoft365/Azure Active Director and email security platforms (e.g. Barracuda, Proofpoint).

f. The successful RESPONDER shall own or have full control and accessibility including content and reporting to the learning management or other equivalent system.

g. The successful RESPONDER shall maintain all cybersecurity products current, with innovative content, and interactive training materials.

h. The cybersecurity courses shall include simulated phishing campaigns to educate the staff against potential cyber threats.

i. The cybersecurity courses shall include a knowledge check at the end of each course to ensure users have gained a practical understanding of cybersecurity risks and how to avoid them.

j. The ideal training system will track and store for a minimum of five (5) years all training activities including the name of the person completing the training, the training sessions completed, the date of the trainings, and the results of any tests administered as part of the training.

    1. Provide reporting at an individual level, entity level, program wide level.
    2. Every Monday provide a training report and every Wednesday a phishing report.

k. Please describe a clear work flow process, describing what process, steps and who is responsible for every stage of the service?

    1. Describe fully how this is to be accomplished.

l. Please describe the respondents support best practices, utilizing technology and techniques to best test the clients network?

    1. Describe fully how this is to be accomplished.

m. Please describe the respondents efforts to maintain client data privacy and security?

    1. Describe fully how this is to be accomplished.

n. Please describe the respondents uptime guarantees and commitment to a level of service that fall within requested metrics.

    1. Describe fully how this is to be accomplished.

2. ~~Security Awareness Notifications~~ (~~remove this section as~~ Underwriting team handles)

a. The successful RESPONDER will provide the FUNDs' members with regular (i.e., ~~monthly) email reminders and notifications on cyber security and other relevant timely~~

~~information regarding recent cyber security threats and how to manage those threats.~~

~~b. The successful RESPONDER will provide the FUNDs' members with regular (i.e., monthly) email reminders regarding the regular updating of anti-virus software and, on an as "needed basis", provide notification to the members of major network software updates (i.e. Microsoft) when released by the manufacturer.~~

~~c. The successful RESPONDER will provide the FUNDs' members with informational posters and/or publications that serve as reminders to members' employees of the need for cyber security.~~

3. Phishing ~~Assessments~~ Simulation Program

a. The successful RESPONDER will offer a process to ascertain the FUNDs' members' vulnerability to "phishing" emails or attacks no less than monthly. RESPONDER should have the capability for more frequent campaigns (bi-weekly or continuous) if requested. The testing process shall be available to all registered users of the training system on an ongoing basis using multiple different phishing simulated emails for the length of this contract.

b. The phishing assessment process shall include an educational component targeted toward those users who fail the phishing email test. Those users who fail the phishing test shall receive automatic remedial training within 15 minutes of the test.

1. The phishing campaign templates shall be customized to match the roles and responsibilities of the intended audience (i.e. – Finance, Human Resources, Information Technology team, etc.), which will include phishing scenarios of varying complexity for each user through multiple attack vectors such as links, attachments and credential harvesting. The campaigns should vary in levels of difficulty.

2. ~~Monthly~~ Phishing reports shall be provided near real-time reporting **(≤ 24 hours)** ~~after each phishing campaign~~. The reports shall include email delivery status (delivered, blocked, quarantined), email opens, credential submission, "click" rates and types of scenarios for each individual, grouped by department or the municipality.
3. The phishing campaign emails shall validate that phishing emails pass SPF, DKIM and DMARC and provide evidence of delivery outcomes.

4. The service shall include:

a. Fully managed email phishing campaigns, managed by successful responder.
b. Quarterly user security training campaigns.
   1. Notify point of contacts when a phishing test will be issued along with the sample phishing
c. Authentic simulated email phishing template library.
d. Comprehensive library of remedial training content.
e. Client dashboard for visibility into campaign details and user scores.
f. Consult with the Client (Executive Director, Deputy Executive Director and Planning Consultant) ~~contact~~ on a ~~quarterly~~ monthly basis to review the program and setup new trainings.
g. The ability to send weekly email reminder notifications to end users that have not completed training.
h. Meet the following percentage timetable requests – phishing reporting latency: (**≤ 24 hours**), Remediation assignment **(≤ 15 minutes)**, Platform uptime **(≥ 99.9%)** and critical issue response **(≤ 4 hours).**
i. Offer benchmarking capabilities to the FUND so comparisons can be made between individual joint insurance funds to the municipal excess liability joint insurance fund and the national standard of similar entities.
j. Confirmation of whitelisting is the responsibility of the vendor to ensure that simulated phishing emails bypass security filters and reach Fund members' inboxes.

5. Reporting & Governance

a. The responder shall provide monthly reports summarizing Training compliance, Phishing performance, participate in monthly program review meetings and provide recommendations for program improvement.

6. Ownership of Records

a. All records and data of any kind relating to the FUND shall belong to the FUND and shall be surrendered to the FUND upon expiration or termination of this Agreement. At all times during the term of this Agreement and for a period of five (5) years from the date of final payment, the FUND, its appointed officials and other designated representatives, as authorized by the FUND, shall have access to records and files maintained by the SERVICE PROVIDER for the FUND during normal business hours. Furthermore, such records, books, and files relating to the operation and business of the FUND are the property of the FUND, regardless of site stored. Information released to the SERVICE PROVIDER by the FUND for the purpose of performing the services as outlined herein shall be used only in connection with the performance of said duties. In addition, Records must be made available to the state office of comptroller upon request.

7. Users per Joint Insurance Fund

a. The below listed Joint Insurance Funds are an approximation and reflective of full time and part time employees for price response:

JIF	Sum FT	Sum PT	Sum Police	Sum JIF
ACM	3,171	4,125	992	8,288
BER	2,602	3,616	929	7,147
BURLCO	1,185	829	458	2,472
CAM	3,141	2,119	959	6,219
CNTRL	3,401	2,460	1,036	6,897
FRESP	309	993	-	1302
MID JERSEY	1,290	1,119	400	2,809
MON	2,526	3,966	919	7,411
MOR	3,501	3,615	1,129	8,245
NJPHA	1,579	512	-	2,091
NJSI	975	876	224	2075
NJUA	2,361	544	-	2,905
OCE	3,499	3,267	1,167	7,933
PAIC	879	1,441	199	2519
PMM	613	402	216	1231
SBER	2,205	2,200	885	5,290
SBEX	1,883	1,287	442	3,612
SBMU	905	985	300	2190
TRICO	2,444	1,813	815	5,072
Total	**38,469**	**36,169**	**11,070**	**85,708**

8. Pricing Response

a. Vendors in their price response will be required to provide a price per user, reflective of the indicated range. The number of users are an approximation and may be accurate to a greater or lesser amount than indicated. The final cost proposal and agreement will be based upon the average price per user as indicated.

b. Per user Phishing and Training price for the JIF's as follows

c. Price response 1
   1. 0 -30,000 users

d. Price response 2
   1. 0-40,000 users

e. Price response 3
   1. 0-50,000 users

f. Price response 4
   1. 0-60,000 users

g. Price response 5
   1. 0-70,000 users

h. Price response 6
   1. 0-80,000 users

i. Price response 7
   1. 0-90,000 users

j. Price response 8
   1. 90,000+ users

k. Average price response

9. Method of award

a. This procurement is being conducted as a competitive contract consistent with NJSA 40A:11-4.1 et. Seq., accordingly, the respondent will be appointed who is deemed to be the most advantageous, price and other factors considered.

b. The weights of the evaluation shall be announced at opening:

   1. Technical _____%
   2. Managerial _____%
   3. Cost _____%
   4. Questions located in the sample rater sheet should be addressed thoroughly in the response.

c. The fund reserves the right to award in any combination of a one (1) to three (3) year term at the discretion of the Fund Commissioners.

10. Questions

a. All questions shall be submitted through the online procurement portal at www.bidnetdirect.com//njcyberjif

11. The summary report as required by law shall be posted on www.bidnetdirect.com//njcyberjif at least 48 hours prior to any action by the board of commissioners.

List Date: July X, 2026

CYBER EXTERNAL SCANNING VENDOR

CC# 26-02
July XX, 2026, at 1:00P.M.

New Jersey Cyber Risk Management Fund
9 Campus Drive, Suite 216
Parsippany, NJ 07054

CYBER EXTERNAL SCANNING VENDOR

1. External Vulnerability Assessments

The vendor will conduct their activities in concordance with the regulations set forth in the Computer Fraud and Abuse Act 9-48.000. No testing will be performed outside of the limited scope as defined in the RFP.

a) The successful RESPONDER will perform ~~monthly~~ no less than weekly port and vulnerability scanning on all public IP Addresses, Domain and Subdomains, Domain Name records, URLs, Web Applications, VPN and remote access portals and email gateways. Detec unknown or "shadow IT" assets and newly exposed systems within 24 hrs. No testing which would be considered invasive or in any way disruptive to normal network operations will be performed. If requested provide continuous or rolling scanning.

b) The successful RESPONDER will provide, at a minimum, monthly external vulnerability scanning reports that are password protected or encrypted to each member identifying the vulnerability, color coded severity risk score.

c) The successful RESPONDER will immediately notify the members of any vulnerabilities that have a high or critical severity score, as well as recommendations for correcting the deficiency. Confirm exploitability and false positive elimination. Automated scan results alone are not acceptable.

Vulnerability Mapping and Penetration – The successful RESPONDER will on a monthly basis, identify vulnerabilities in external in-scope hosts in the perimeter provided by the member. They will also prepare a monthly report which will be uploaded to a secure portal; access to the portal shall be limited to designated personnel for each member and fund administrator.

This includes identifying and reporting on:
• Vulnerabilities
  - Name the application-level vulnerabilities (Webs apps, OWASP 10, etc.)
• Require mapping to Common Vulnerability Scoring System
• Missing security patches
• Externally visible sub-domains & email addresses
• Web services linking to malicious content
• Misconfigured externally visible devices
• Potentially unwanted or unmanaged software
• External IP communicating with any botnet-infected systems
• Open Ports

The successful responder shall at a minimum provide a ~~quarterly~~ monthly report outlining key findings, color-coded risk levels, and recommendations to the Fund Administrators office. The report should have an executive summary and detailed findings that are easily integrated into ticketing/incident tracking systems hosted by the members. Reporting should also include a trend analysis and benchmarking for agency against the entire MEL and industry standards.

d) The RESPONDER must provide as part of its response an interactive portal for the Fund to

be capable of providing for public facing IP addresses of members or suitable alternative data submission method adequately described in response proposal.

e) The RESPONDER will be responsible for coordinating with the Entity Contact, or their designee to ensure Entity understands what data is required and how to manage portal.

f) The RESPONDER as part of its service will provide for baseline security scanning assessments. The results will be reviewed by the professional staff of the responder and provide an understandable summary of scanning efforts of the Fund and its members.

g) All scanning assessments will be conducted as a monthly service. The RESPONDER will provide for detailed resumes and qualifications of key staff.

h) The RESPONDER if requested should be able to disclose any relevant certifications (i.e. CISSP, ISO 27001, GEVA, CompTIA PenTest+, etc.).

i) The RESPONDER will ensure that the questions in the attached rater sheet are adequately addressed in any response to this competitive contract.

j) Responder shall maintain all records, information, and sensitive data in a manner consistent with best practices of confidentiality, insuring the integrity of the clients information.

- Describe fully how this is to be accomplished.

k) Please describe a clear work flow process, describing what process, steps and who is responsible for every stage of the service? In addition to describing what is in place to address escalation/support process for technical issues.

- Describe fully how this is to be accomplished.

l) Please describe the respondents support best practices, utilizing technology and techniques to best test the clients network?

- Describe fully how this is to be accomplished.

2. Service Levels:

a) The responder shall meet Critical vulnerability notification: ≤ 24 hours, High vulnerability notification: ≤ 48 hours and Validation of critical findings: ≤ 72 hours.

3. **Ownership Of Records:** All records and data of any kind relating to the FUND shall belong to the FUND, and shall be surrendered to the FUND upon expiration or termination of this Agreement. At all times during the term of this Agreement and for a period of five (5) years from the date of final payment, the FUND, its appointed officials and other designated representatives, as authorized by the FUND, shall have access to records and files maintained by the SERVICE PROVIDER for the FUND during normal business hours. Furthermore, such records, books, and files relating to the operation and business of the FUND are the property of the FUND, regardless of site stored. Information released to the SERVICE PROVIDER by the FUND for the purpose of performing the services as outlined herein shall be used only in connection with the performance of said duties. In addition, Records must be made available to the state office of comptroller upon request.

4. **Entities per Joint Insurance Fund**
   a) The below listed Joint Insurance Funds are reflective of entities per joint insurance fund for price response:

JIF	**Entities**
ACM	41
BER	38
BURLCO	28
CAM	39
CNTRL	15
FRESP	32
MID JERSEY	12
MON	41
MOR	45
NJPHA	89
NJSI	5
NJUA	73
OCE	31
PAIC	21
PMM	5
SBER	23
SBMETRO	11
SBMU	10
TRICO	38
Total	**597**

   b) **Pricing Response**
      - The vendor is to respond per entity. The amount of public facing IP addresses cannot be considered as part of the response. Public facing IP addresses are to be inclusive of all.
      - Per entity vulnerability scanning as follows

   c) Pricing response 1 - 0-452 member entities
   d) Pricing response 2 - 0-490 member entities
   e) Pricing response 3 - 0-597 member entities
   f) Average of all pricing response per entity.

5. Method of award

a) This procurement is being conducted as a competitive contract consistent with NJSA 40A:11-4.1 et. Seq., accordingly, the respondent will be appointed who is deemed to be the most advantageous, price and other factors considered.

b) The weights of the evaluation shall be announced at opening:

- Technical _____%
- Managerial _____%
- Cost _____%
- Questions located in the sample rater sheet should be addressed thoroughly in the response

c) The fund reserves the right to award in any combination of a one (1) to three (3) year term at the discretion of the Fund Commissioners.

6. Questions

a) All questions shall be submitted through the online procurement portal at www.bidnetdirect.com//njcyberjif

7. The summary report, as required by law shall be posted on www.bidnetdirect.com//njcyberjif at least 48 hours prior to any action by the board of commissioners.

Excerpt from Princeton Strategic Communications Report
on 1st Quarter 2026 Cyber Website usage

Cyber JIF Website

The Cyber JIF website averaged 600 users per month since January, and 4,100 pageviews. Users visit an average of 2 pages per session, and spend around :34 seconds on each page. The Cyber site reached a milestone this month, reaching a total of 300 request forms for access having been filled out since the launch of the secured documents page. Not all 300 have been granted access, but the number shows the popularity of the site.

All three websites are accessed primarily, more than 85%, from desktop computers. MSI experiences the highest mobile phone access rate, 14.5%, out of the websites.

AI Chatbot: Discussions are currently underway to add an AI Chatbot to the MSI website. If approved, this addition may start over the summer due to the ramp-up time/details involved. This will also directly involve members of the MSI team to help develop key questions, answers, and lists of resources to train the chatbot and test its effectiveness. The chatbot will also be able to pull resources from the MEL site to answer questions.

Cyber JIF Website	January 2026	February 2026	March 2026	YTD 2026
Website Users	768	547	586	1,851
Pageviews	1,724	1,172	1,266	4,162
Pages/Session	2.24	2.14	2.16	2.25
Event Count	5,430	3,715	3,937	13,112
Session Duration	:35	:30	:33	:34

Cyber JIF	Top Pages Viewed
Jan-Mar.	Home, Login, Documents, Resources, Secure Documents, Governance, Registration, About, News articles on Chrome and Phishing

From: Jaine Testa
To:
Subject: NJ Cyber Risk Management Fund Educational Series – June & August – Registration information
Date: Monday, June 15, 2026 5:43:48 PM

The email below regarding the Cyber JIF educational series, was sent Monday to all PERMA and RPA JIF fund commissioners and risk managers.

Memo to: Fund Commissioners & Risk Management Consultants (via bcc)
Cyber Affiliated Joint Insurance Funds

From: Edward Cooney, Underwriting Manager

Subject: Cyber JIF Educational Series – June 23rd at 10:00 am & August 5th at 10:00 am

We are pleased to announce the 1st and 2nd in the cyber educational series sponsored by the NJ Cyber Risk Management Fund. Below is the link to register for the June 23rd session.

The topic for the August 5th seminar will be "Cybersecurity Insights in 2026: Emerging Risks, JCMI Banking Controls, and Framework Fundamentals". Link for August session will be sent at a later date.

June 23, 2026 at 10:00 am:
Topic: Artificial Intelligence

June registration link:
https://permainc.zoom.us/webinar/register/WN_ndcbZpObTJSg2cECISZUtg

NEW JERSEY CYBER RISK MANAGEMENT FUND

FINANCIAL FAST TRACK REPORT

March 31, 2026

ALL YEARS COMBINED

	YTD CHANGE	PRIOR YEAR END	FUND BALANCE
UNDERWRITING INCOME	**1,723,565**	**19,597,602**	**21,321,167**
CLAIM EXPENSES			
Paid Claims	71,411	1,533,301	**1,604,713**
Case Reserves	12,304	320,714	**333,019**
IBNR	25,847	2,309,559	**2,335,406**
Recoveries	-	(24,235)	**(24,235)**
Total Claims	**109,562**	**4,139,340**	**4,248,902**
EXPENSES			
Excess Premiums	520,251	6,679,327	**7,199,578**
Administrative	426,285	3,106,523	**3,532,808**
Total Expenses	**946,535**	**9,785,850**	**10,732,386**
UNDERWRITING SURPLUS	**667,467**	**5,672,412**	**6,339,879**
INVESTMENT INCOME	88,836	628,082	**716,918**
DIVIDEND EXPENSE	-		**-**
OPERATING SURPLUS	**756,303**	**6,300,494**	**7,056,797**
			-
SURPLUS	**756,303**	**6,300,494**	**7,056,797**

SURPLUS (DEFICITS) BY FUND YEAR

2023	**33,194**	**3,231,248**	**3,264,442**
2024	**99,920**	**1,857,371**	**1,957,291**
2025	**208,677**	**1,211,875**	**1,420,552**
2026	**414,511**		**414,511**
TOTAL	**756,303**	**6,300,494**	**7,056,797**
TOTAL CASH			**10,267,557**

CLAIM ANALYSIS BY FUND YEAR

	YTD CHANGE	PRIOR YEAR END	FUND BALANCE
FUND YEAR 2023			
Paid Claims	-	764,559	**764,559**
Case Reserves	-	(0)	**(0)**
IBNR	(6,933)	27,984	**21,051**
Recoveries	-	(24,235)	**(24,235)**
Total Claims	**(6,933)**	**768,308**	**761,375**
FUND YEAR 2024			
Paid Claims	(25,443)	418,033	**392,590**
Case Reserves	(7,402)	77,798	**70,396**
IBNR	(41,413)	720,219	**678,806**
Recoveries	-	-	**-**
Total Claims	**(74,257)**	**1,216,049**	**1,141,792**
FUND YEAR 2025			
Paid Claims	96,854	350,710	**447,563**
Case Reserves	19,706	242,917	**262,623**
IBNR	(300,112)	1,561,356	**1,261,244**
Recoveries	-	-	**-**
Total Claims	**(183,553)**	**2,154,983**	**1,971,430**
FUND YEAR 2026			
Paid Claims	-		**-**
Case Reserves	-		**-**
IBNR	374,305		**374,305**
Recoveries	-		**-**
Total Claims	**374,305**	**-**	**374,305**
COMBINED TOTAL CLAIMS	**109,562**	**4,139,340**	**4,248,902**

'This report is based upon information which has not been audited nor certified by an actuary and as such may not truly represent the condition of the fund.

Cyber Risk Management Fund
Loss Ratios By JIF
Valued as of : 5/31/2026

Fund Year 2026

JIF Name	Loss Fund	# of Claims	Total Paid (Net Recoveries)	Total Incurred	Loss Ratio	Profit/Loss
ATL	186,122	1	0	25,000	13.43%	161,122
BER	232,454	1	0	0	0.00%	232,454
BURL	157,369	0	0	0	0.00%	157,369
CAM	211,685	1	0	0	0.00%	211,685
CNTRL	141,010	0	0	0	0.00%	141,010
FRESP	108,675	0	0	0	0.00%	108,675
MID JERSEY	110,284	0	0	0	0.00%	110,284
MON	214,939	2	0	0	0.00%	214,939
MOR	276,195	3	11,070	25,000	9.05%	251,195
NJPHA	360,523	1	0	0	0.00%	360,523
NJSI	25,052	0	0	0	0.00%	25,052
NJUA	300,001	1	0	0	0.00%	300,001
OCE	168,920	0	0	0	0.00%	168,920
PAIC	92,023	0	0	0	0.00%	92,023
PMM	31,136	0	0	0	0.00%	31,136
SBER	151,522	1	5,000	25,000	16.50%	126,522
SBEX	71,582	0	0	0	0.00%	71,582
SBMU	74,396	4	0	0	0.00%	74,396
TRICO	190,194	0	0	0	0.00%	190,194
Totals	**3,104,082**	**15**	**16,070**	**75,000**	**2.42%**	**3,029,082**

Fund Year 2025

JIF Name	Loss Fund	# of Claims	Total Paid (Net Recoveries)	Total Incurred	Loss Ratio	Profit/Loss
ATL	182,676	3	212,894	330,399	180.87%	(147,723)
BER	210,315	1	0	0	0.00%	210,315
BURL	142,390	1	0	0	0.00%	142,390
CAM	191,563	1	0	0	0.00%	191,563
CNTRL	120,089	0	0	0	0.00%	120,089
FRESP	92,730	0	0	0	0.00%	92,730
MID JERSEY	99,779	2	0	0	0.00%	99,779
MON	194,108	2	16,388	25,000	12.88%	169,108
MOR	256,285	1	0	0	0.00%	256,285
NJPHA	328,319	1	7,835	25,000	7.61%	303,319
NJSI	29,427	0	0	0	0.00%	29,427
NJUA	271,418	1	38,218	75,000	27.63%	196,418
OCE	152,840	2	309,246	350,000	229.00%	(197,160)
PAIC	83,382	1	0	0	0.00%	83,382
PMM	28,173	0	0	0	0.00%	28,173
SBER	137,102	2	62,600	100,000	72.94%	37,102
SBEX	64,793	0	0	0	0.00%	64,793
SBMU	67,319	1	0	0	0.00%	67,319
TRICO	176,019	2	17,128	25,000	14.20%	151,019
Totals	**2,828,727**	**21**	**664,308**	**930,399**	**32.89%**	**1,898,328**

Fund Year 2024

JIF Name	Loss Fund	# of Claims	Total Paid (Net Recoveries)	Total Incurred	Loss Ratio	Profit/Loss
ATL	170,274	4	84,362	84,362	49.54%	85,913
BER	196,043	2	50,894	75,000	38.26%	121,043
BURL	132,720	0	0	0	0.00%	132,720
CAM	178,532	3	109,140	133,613	74.84%	44,919
CNTRL	111,904	2	230,970	248,441	222.01%	(136,537)
FRESP	89,012	0	0	0	0.00%	89,012
MID JERSEY	71,009	1	0	0	0.00%	71,009
MON	180,925	1	0	0	0.00%	180,925
MOR	232,591	0	0	0	0.00%	232,591
NJPHA	302,412	0	0	0	0.00%	302,412
NJSI	27,431	0	0	0	0.00%	27,431
NJUA	245,893	1	48,783	48,783	19.84%	197,111
OCE	142,443	2	0	0	0.00%	142,443
PAIC	84,330	1	0	0	0.00%	84,330
PMM	26,256	0	0	0	0.00%	26,256
SBER	127,795	2	0	0	0.00%	127,795
SBEX	60,335	0	0	0	0.00%	60,335
SBMU	62,745	0	0	0	0.00%	62,745
TRICO	167,085	3	52,420	52,420	31.37%	114,665
Totals	**2,609,735**	**22**	**576,568**	**642,618**	**24.62%**	**1,967,117**

Fund Year 2023

JIF Name	Loss Fund	# of Claims	Total Paid (Net Recoveries)	Total Incurred	Loss Ratio	Profit/Loss
ATL	183,567	2	0	0	0.00%	183,567
BER	177,293	1	0	0	0.00%	177,293
BURL	127,278	0	0	0	0.00%	127,278
CAM	173,376	0	0	0	0.00%	173,376
CNTRL	79,172	1	175,324	175,324	221.45%	(96,152)
FRESP	107,280	0	0	0	0.00%	107,280
MID JERSEY	63,258	1	0	0	0.00%	63,258
MON	182,479	1	33,278	33,278	18.24%	149,202
MOR	211,892	0	0	0	0.00%	211,892
NJPHA	319,465	0	0	0	0.00%	319,465
NJSI	24,246	0	0	0	0.00%	24,246
NJUA	236,526	0	0	0	0.00%	236,526
OCE	142,702	1	0	0	0.00%	142,702
PAIC	91,160	0	0	0	0.00%	91,160
PMM	21,575	0	0	0	0.00%	21,575
SBER	111,310	3	391,820	391,820	352.01%	(280,510)
SBEX	55,018	0	0	0	0.00%	55,018
SBMU	47,620	0	0	0	0.00%	47,620
TRICO	169,182	2	356,935	356,935	210.98%	(187,753)
Totals	**2,524,399**	**12**	**957,356**	**957,356**	**37.92%**	**1,567,043**

NEW JERSEY CYBER RISK MANAGEMENT FUND
BILLS LIST

Resolution No. 33-26 **JUNE 2026**

WHEREAS, the Treasurer has certified that funding is available to pay the following bills:

BE IT RESOLVED that the New Jersey Cyber Risk Management Fund's Executive Board, hereby authorizes the Fund treasurer to issue warrants in payment of the following claims; and

FURTHER, that this authorization shall be made a permanent part of the records of the Fund.

FUND YEAR 2025

Vendor Name	Comment	Invoice Amount
QUAL-LYNX	2025 BANKING SERVICES 06/26	6,000.00
		6,000.00
NISIVOCCIA LLP	2025 AUDIT BILLING 06/26	26,010.00
		26,010.00
	Total Payments FY 2025	**32,010.00**

FUND YEAR 2026

Vendor Name	Comment	Invoice Amount
CB CLAIMS LLC	CLAIMS ADMIN FEE 06/26	2,210.83
		2,210.83
QUAL-LYNX	BANKING SERVICES FOR 05/26	500.00
QUAL-LYNX	BANKING SERVICES FOR 04/26	500.00
QUAL-LYNX	BANKING SERVICES FOR 06/26	500.00
QUAL-LYNX	BANKING SERVICES FOR 01/26	500.00
QUAL-LYNX	BANKING SERVICES FOR 02/26	500.00
QUAL-LYNX	BANKING SERVICES FOR 03/26	500.00
		3,000.00
PERMA RISK MANAGEMENT	POSTAGE 05/26	8.88
PERMA RISK MANAGEMENT	ADMIN FEE 06/26	11,054.25
		11,063.13
THE ACTUARIAL ADVANTAGE	ACTUARY FEES 06/26	2,210.83
		2,210.83
ARTHUR J GALLAGHER LLC dba	DEPUTY ADMINISTRATOR 06/26	4,421.67
ARTHUR J GALLAGHER LLC dba	EXEC DIR. COOR. FEES Q2 2026 06/26	7,101.93
		11,523.60
RISK & LOSS MANAGERS, INC	PLANNING CONSULTANT Q2 2026 06/26	3,979.50
RISK & LOSS MANAGERS, INC	LOCAL COORDINATOR Q2 2026 06/26	1,810.00
		5,789.50
CHARLES CUCCIA	TREASURER FEE 06/26	2,210.83
		2,210.83
PERMA RISK MANAGEMENT SERVICES	LOCAL EXEC DIR. COORD. Q2 2026	29,880.25
		29,880.25
CONNER STRONG AND BUCKELEW	UNDERWRITING MGR 06/26	4,421.67
		4,421.67
CHERTOFF GROUP LLC	CYBER PROGRAM SUPPORT 4/24/26-5/23/26	5,100.00
		5,100.00
LARACY ASSOCIATES, LLC	INDEPENDENT ACCOUNTANT FEES 06/26	625.00
		625.00
PL SERVICES, LLC AKA PEGAS	LOCAL COORDINATOR Q2 2026 06/26	2,684.50
		2,684.50

THE CANNING GROUP LLC	QPA SERVICES INV 2026-06	1,326.50
		1,326.50
CONNER STRONG & BUCKELEW	IND. HARBOR TECH E&O RENEWAL 5/26-5/27	25,640.00
		25,640.00
HOLIDAY INN OF EAST WINDSOR	2ND DEPOSIT FOR EVENTS 10844-10845	6,000.00
		6,000.00
	Total Payments FY	**113,686.64**
	TOTAL PAYMENTS ALL FUND YEARS	**145,696.64**

Chairperson

Attest:

_____ Dated: _____

I hereby certify the availability of sufficient unencumbered funds in the proper accounts to fully pay the above claims

Treasurer

APPENDIX I

NEW JERSEY CYBER RISK MANAGEMENT FUND
OPEN MINUTES
MAY 21, 2026
VIA TELECONFERENCE – 1:30 PM

Acting Chair Brewer called the meeting to order and read the statement of compliance open public meeting act, followed by the Pledge of Allegiance.

ROLL CALL OF 2026 FUND COMMISSIONERS

Joy Tozzi - Chair	East Windsor - Mid-Jersey JIF	Absent
Adam Brewer - Secretary	Pequannock Township – Morris JIF	Present
Megan Champney Kweselait	City of Summit- Suburban Municipal JIF	Present
James Gant	Sea Girt Borough – Monmouth JIF	Absent
Michael Mevoli	Borough of Brooklawn - Camden JIF	Present
Bernard Rutkowski	Toms River MUA - NJUA JIF	Absent
Marc Schrieks	Lodi Borough – South Bergen JIF	Present
James Pacanowski	Ventnor City, Atlantic JIF	Present
Corey Gallo	Bergenfield - Bergen JIF	Present
Erin Provenzano	Delanco- Burlco JIF	Present
Casey Wagner	Woodbridge - Central JIF	Present
Alan Pine	Mount Laurel Twp. FD#1 – FIRST JIF	Present
Matthew von der Hayden	Stafford Township – Ocean JIF	Present
Frank Elenio	Ridgefield Borough – PAIC JIF	Absent
Kevin Aberant	Moorestown - PMM JIF	Present
John Clarke	Princeton Housing Authority- NJPHA JIF	Present
James Ulrich	Clark Township – NJSI JIF	Present
Gary Jeffas	Secaucus – Suburban Metro JIF	Present
Michael Razze	Pittman Borough - Trico JIF	Present

PROFESSIONALS PRESENT:

Executive Director/Admin.	PERMA Risk Management Services **Cathleen Kiernan, Joseph Hrubash,**
Deputy Executive Director	Risk Program Administrators **Kamini Patel**
Claims Adjustor	CB Claims LLC **Chris Botta, Esq.**
Attorney	Dorsey & Semrau **Frederick Semrau, Esq.**
Underwriting Manager	Conner Strong & Buckelew **Edward Cooney**
Cyber Security Training	**Xcitium** **Alex Leonard**
Treasurer	**Chuck Cuccia**

ALSO PRESENT:
Joseph Capano, Cliffside Park Housing Authority, Alternate Fund Commissioner, NJPHA JIF
Justin Macko, Sea Girt Borough, Alternate Fund Commissioner, Monmouth JIF
Diane Ambrosio, Ocean Township
Mathew T. McArow, GJEM – Otterstedt Insurance Agency
Don Sciolaro, World Insurance Associates LLC
Tom Merchel, Conner Strong & Buckelew
Jaclyn Lindsey, Conner Strong & Buckelew
Katie Walters, Conner Strong & Buckelew
Jonathon Tavares, Conner Strong & Buckelew
Dave Vozza, The Vozza Agency
Charles Casagrande, Danskin Insurance Agency
John Casagrande, Danskin Insurance Agency
Alison Kelly, Danskin Insurance Agency
Robin Racioppi, North American Insurance Agency
Brad Stokes, Perma Risk Management Services
Steve Sacco, Perma Risk Management Services
Pauline Kontomanolis, Perma Risk Management Services
Robyn Walcoff, Perma Risk Management Services
Zareena Majeed, Perma Risk Management Services
Brandon Tracy, Perma Risk Management Services

MINUTES: Included in the agenda were the open and closed minutes of March 19, 2026.

MOTION TO APPROVE MARCH 19, 2026 OPEN MINUTES:

Moved:	Commissioner Shrieks
Second:	Commissioner Clarke
All in favor:	Unanimous

Executive Director said there was no correspondence to review.

CLAIMS COMMITTEE: The Committee met virtually at 10:00am before the Board meeting to discuss two Payment Authority Requests (PARs).

MOTION TO APPROVE THE PARS AS RECOMMENDED BY THE CLAIMS COMMITTEE.

Moved:	Commissioner Mevoli
Second:	Commissioner Pacinowski
Vote:	15 Ayes -0 Nays

3RD PARTY RISK ASSESSMENT TOOL: Assistant Executive Director said the underwriting Manager submitted a revised 3rd Party Risk Assessment Tool in March and was asked to see if he could revisit to reduce some redundancies, but he was not able to accommodate as there was too much concern about vendors changing their controls down the line and the Cyber Fund not wanting to recommend any particular vendors. Assistant Executive Director Kiernan said this tool can be found on the Cyber JIF website and helps assess the security controls implemented by a third-party vendor. Mr. Cooney reminded members that the tool was developed in conjunction with the Operations Committee and The Chertoff Group.

MOTION TO APPROVE THE AMENDED 3RD PARTY RISK ASSESSMENT TOOL.

Moved:	Commissioner Champney
Second:	Commissioner Clarke
Vote:	14 Ayes -1 Nay

OPERATIONS COMMITTEE: The Committee met virtually on May 18th at 11:30 a.m.; included in the agenda were the minutes. The Committee discussed the following:

CYBER CLAIMS: At the March 19th Fund meeting, Underwriting Manager reported members have experienced difficulties complying with local public contract laws and/or organizing their council quickly enough to rapidly engage cyber legal counsel and forensic vendors.

Recognizing this challenge, the Underwriting Manager worked on a solution. Specific to the cyber legal counsel, we have come to an agreement in principle with Mullen Coughlin on a solution through a Master Service Agreement. Underwriting Manager consulted with the Fund Attorney and several QPAs and presented a copy of the agreement to the operations committee. The committee agreed to present it to the Board of Fund Commissioners for approval. Included in the agenda was the agreement. Commissioner Pacanowski asked for clarification on the agreement under item 7.B. Outside consultants and other vendors specifically concerning vendors that are procured to rebuild the township network and services. Mr. Cooney said the process of obtaining those services are outside the scope of the agreement and will remain the same and AXA XL has been helpful making sure some of the additional outside-the-norm expenses get paid.

MOTION TO APPROVE THE MASTER SERVICE AGREEMENT WITH MULLEN COUGHLIN, LLC AS PRESENTED.

Moved: Commissioner Pacanowski
Second: Commissioner Schrieks
Vote: 15 Ayes -0 Nays

AMENDING DEDUCTIBLE CONTROLS: At the March 19th Fund meeting, the Board of Fund Commissioners were presented with amended deductible control options where basic deductible is reduced to $25,000, intermediate the deductible is reduced to $0 and advanced there is a premium reduction of 20%.

Committee reviewed the proposed amendments to the deductible incentive structure and recommend adopting effective June 1, 2026. In addition, Committee recommends the advanced premium incentive of 20% be effective retroactive to January 1, 2026 for those members fully compliant and have provided supporting documentation to the Underwriting Manager. Assistant Executive Director said the compliance review would be annual.

Included in the agenda was Resolution 29-26 Amending Deductible Controls for 2026 Renewal of Excess Cyber Coverage drafted by the Fund Attorney.

MOTION TO APPROVE RESOLUTION 29-26 AMENDING DEDUCTIBLE CONTROLS FOR 2026 RENEWAL OF EXCESS CYBER COVERAGE

Moved: Commissioner Shrieks
Second: Commissioner Champney
Vote: 15 Ayes -0 Nays

EDUCATIONAL PROGRAMS:

CYBER JIF ACCREDITATION PROGRAM: Executive Director provided an update on the accreditation program that was approved by the Board of Fund Commissioners at the March 19th Fund meeting. The program has been tentatively scheduled for Friday October 2nd and Friday October 9th from 9am – 2pm at the National Conference Center. Underwriting Manager will begin refining the program and finalizing speakers. Executive Director's office will send out a "save the date".

2026 WEBINAR SERIES: Underwriting Manager provided an update on the Cyber Educational Series noting the (1) Artificial Intelligence and (2) Cybersecurity Insights in 2026: Emerging Risks, JCMI Banking Controls, and Framework Fundamentals are scheduled for Tuesday June 23, 2026 at 10am and Wednesday, August 5th at 10am. Registration links will be sent following the meeting.

RISK CONTROL SERVICES: In March, the board appointed a task force to prepare the Competitive Contracting RFP for cyber training/phishing simulation & vulnerability scanning; current contract expires in September. The task force, comprised of the Executive Director, Deputy Executive Director, Planning Consultant and Underwriting Manager have met twice to review the scope of services and will submit their draft to the Chertoff Group and several municipal IT professionals prior to presenting a final draft to the operations committee. Executive Director expects the RFPs to be issued in July.

CYBER RISK ALERT: OUTSOURCED VENDOR BREAK: Committee discussed a notice that was issued by the Underwriting Manager via email alerting members and risk managers of a breach to SDL, aka GovPilot, a common outsourced vendor used by large numbers of members. Underwriting Manager is coordinating with AXA XL to set up a mass report for affected members. Members are encouraged to call the AXA XL hotline to begin working through actual or potential issues. The email was included in the agenda.

TECHNOLOGY E&O COVERAGE OPTION: Underwriting Manager renewed this coverage for a short-term expiring 1/1/27 for Ho-Ho-Kus Borough, Vineland Housing Authority, City of Camden, Woodbridge Township, Allentown Borough, Oceanport Borough, Madison Borough and Riverside Township.

CYBER RISK ALERT: Fund office distributed a bulletin via email addressing the potential impact on cyber risks resulting from the situation in Iran, provided to us by the JIF's partner, The Chertoff Group. The email was included in the agenda.

FINANCIAL DISCLOSURES: All JIF Commissioners and required professionals completed the online filing of the Financial Disclosure forms by the April 30th filing deadline.

AUDITOR & ACTUARY YEAR-END REPORTS: The financial audit for the period ending December 31, 2025 will be ready for review and approval at the June meeting and will be filed with the Departments of Insurance and Community Affairs by the June 30th deadline.

DUE DILIGENCE: The Financial Fast Track report as of March 31, 2026 was included in the agenda and resulted in a surplus in the amount of $7,056,797. The loss ratio report as of March 31, 2026 was also included in the agenda.

NEXT MEETING: The next Cyber JIF meeting is scheduled for May 21, 2026 at 1:30 PM via audio / video teleconference.

TREASURER: Treasurer asked for a motion to confirm Resolution 30-26 April 2026 Bills List and approve Resolution 31-26 May 2026 Bills list:

April 2026	
2026	$880,196.52
Total	$880,196.52

May 2026	
2025	$1,200.00
2026	$207,476.64
Total	$$208,676.64

MOTION TO ADOPT RESOLUTION 30-26 CONFIRMING THE APRIL 2026 PAYMENTS AND TO ADOPT RESOLUTION 31-26 APPROVING THE MAY 2026 PAYMENS, AS SUBMITTED

Moved: Commissioner Clarke
Second: Commissioner Macko
Roll Call Vote: 15 Ayes - 0 Nays

UNDERWRITING MANAGER: Mr. Cooney reviewed the two bulletin announcements and recommended members distribute the bulletin to their citizens. The first infographic, created at the request of several Commissioners, focuses on scammers impersonating the towns trying to get citizens to do this. It's been going on for a long time, but it's increasing now.

The second bulletin is another story about an attacker that worked their way into the emails of one of our members and while in the emails learned the routine analyzing the Fund's billing communication and as a result were able to use as part of their scam. Underwriting Manager said fortunately it didn't work because the members were well trained.

Mr. Cooney added an announcement about the updated deductibles in the program along with the very specific guidelines for the advanced tier, which is now the premium credit will be distributed.

ATTORNEY: Fund Attorney commended Underwriting Manger on his quick responses on the scam alert and development of the Master Service Agreement. Mr. Semrau said with respect to the scam alert Mr. Cooney and his team were able to issue an alert and announcement within 24 hours, which is important when responding to these events.

Mr. Semrau applauded the Fund Commissioners for their assistance and patience throughout the process and said Mr. Cooney worked diligently through the process. Mr. Semrau recognized from the standpoint of legal counsel and their expertise in this area the agreement is necessary as a retainer-type agreement because anyone who breaks through that privileged type of communication can try to make a claim for a class action type suit, if they can prove that there is a breach.

NEW BUSINESS:

None.

OLD BUSINESS:

Commissioner Jeffas inquired about the SDL breach and Mr. Cooney said a memo went out from PERMA and can forward another copy and recommended the member to precautionarily submit the concern to the Underwriting team so they can get a notice into the insurance company.

PUBLIC COMMENT:

None

CLOSED SESSION: There was not a need for closed session.

MEETING ADJOURNED: 2:17 PM

Brandon Tracy, Assisting Secretary for Adam Brewer, Secretary