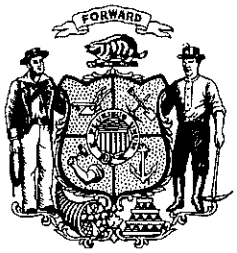
State of Wisconsin

SENATE CHAIR
Alberta Darling

317 East, State Capitol
P.O. Box 7882
Madison, WI 53707-7882
Phone: (608) 266-5830



ASSEMBLY CHAIR
John Nygren

309 East, State Capitol
P.O. Box 8593
Madison, WI 53708-8953
Phone: (608) 266-2343

Joint Committee on Finance

MEMORANDUM

To: Members
Joint Committee on Finance

From: Senator Alberta Darling
Representative John Nygren

Date: March 7, 2017

Re: 14-Day Passive Review Approval – DOA

Pursuant to Sections 9112(1) and 9212(1) of 2013 Wisconsin Act 20, attached is a 14-day passive review request from the Department of Administration, received on March 7, 2017.

Please review the material and notify **Senator Darling** or **Representative Nygren** no later than **Friday, March 24, 2017,** if you have any concerns about the request or if you would like the Committee to meet formally to consider it.

Also, please contact us if you need further information.

Attachments

AD:JN:jm

SCOTT WALKER

GOVERNOR
STATE OF WISCONSIN

February 14, 2017

The Honorable Alberta Darling, Co-Chair
Joint Committee on Finance
317 East, State Capitol
Madison, WI 53702

MAR 07 2017
Jt. Finance

The Honorable John Nygren, Co-Chair
Joint Committee on Finance
309 East, State Capitol
Madison, WI 53702

SUBJECT: Notification of Position and Supplementary Funding Request

Dear Senator Darling, Representative Nygren and Members:

Attached are a request and recommendation for positions and supplementary funding related to an initiative to modernize and integrate agency operations in the Department of Employee Trust Funds. Pursuant to Sections 9112(1) and 9212(1) of 2013 Wisconsin Act 20, the department may request that I create positions or supplement any sum certain appropriation from the public employee trust fund for these purposes. Unless you notify me within 14 working days after the date of this notification letter that a meeting has been scheduled for the Joint Committee on Finance to review the proposed request, I will approve the positions as recommended in the attached memorandum.

Please contact State Budget Director Waylon Hurlburt (266-1035) if you have any questions or if you schedule a meeting to review the proposed position request.

Thank you for your prompt attention to this matter.

Sincerely,

SCOTT WALKER
Governor

Date: 3-7-2017

cc: Members, Joint Committee on Finance

Attachments

P.O. BOX 7863, MADISON, WISCONSIN 53707-7863 • (608) 266-1212 • FAX: (608) 267-8983
WWW.WISGOV.STATE.WI.US

WISCONSIN DEPARTMENT OF
ADMINISTRATION

SCOTT WALKER
GOVERNOR
SCOTT A. NEITZEL
SECRETARY
Office of the Secretary
Post Office Box 7864
Madison, WI 53707-7864
Voice (608) 266-1741
Fax (608) 267-3842
TTY (608) 267-9629

Date: February 7, 2017

To: The Honorable Scott Walker
Governor of Wisconsin

From: Scott A. Neitzel, Secretary
Department of Administration

Subject: Passive Review Request under Sections 9112(1) and 9212(1), 2013 Wisconsin Act 20, from the Department of Employee Trust Funds for Cybersecurity Positions and Supplemental Funding Related to an Initiative to Modernize and Integrate Agency Operations

Request:

The Department of Employee Trust Funds requests the creation of 3.0 FTE SEG computer and Internet security analyst permanent positions and $458,800 SEG in fiscal year 2016-17 and $590,200 SEG ongoing funding, beginning in fiscal year 2017-18, in its general program operations appropriation under s. 20.515(1)(w) to implement and maintain a more robust cybersecurity program.

Background:

A nonstatutory provision was included in 2013 Wisconsin Act 20 that allows the department to request, through a passive review process, supplemental funding and positions to address increasing workload due to the replacement of its benefits administration system and the modernization of its business processes as part of the Transformation, Integration and Modernization (TIM) project. Act 20 allows for the secretary of the department to submit a request to the Governor to supplement any sum certain appropriation from the public employee trust fund or create or abolish FTE positions funded from revenues deposited in the public employee trust fund, if the duties performed by these positions would relate the project. The Governor may approve or modify the request and then shall notify the Joint Committee on Finance of his proposed action. The Committee has 14 working days to schedule a meeting for the purpose of reviewing the request or the position changes proposed by the Governor. The department has the authority to utilize this provision through fiscal year 2018-19.

The department is requesting the following additional funding and FTE position authority:

- 3.0 FTE Computer and Internet Security Analyst Permanent Positions. The department requests $178,800 SEG in fiscal year 2016-17 and $310,200 SEG in ongoing expenditure authority to fund these positions, beginning in fiscal year 2017-18. These positions will be responsible for implementing information technology security activities, collaborating with the Department of Administration's Division of Enterprise Technology on security management, maintaining and optimizing the department's security alert software, improving vulnerability management processes, managing and improving the department's network security by working with the division to ensure that firewalls are properly maintained, managing antimalware software to protect all user workstations and legacy application servers, and routinely testing the department's vulnerability. Cybersecurity staff will need to understand the department's unique business operations and processes. The department's chief information security officer will direct staff in identifying, developing, implementing and maintaining processes to reduce information technology risks.

- Cybersecurity Liability Insurance. The department also requests $150,000 SEG annually for cybersecurity liability insurance. Since commercial general liability and property insurance policies do not include cyberrelated risks in their terms and conditions, the department has been working with the Department of Administration's Bureau of State Risk Management to perform an assessment and analysis of which type of cybersecurity insurance it needs. Cybersecurity liability insurance will provide the department protection against catastrophic financial losses that it may suffer, including costs incurred from data destruction, extortion demands, hacking, denial of service attacks, crisis management activities related to data breaches and legal claims for defamation, fraud and privacy violations.

- Information Technology Audits. Finally, the department requests $130,000 SEG annually for a contract with a third-party expert in data security to perform routine information technology audits. Audit findings will assist the department in identifying critical gaps in data security, inform updated departmental policies and procedures, and direct the projects and duties of cybersecurity staff.

The goal of the department's TIM initiative is to efficiently upgrade information technology systems and modernize business processes that are required to administer all of the benefit programs for state and local government employees. Accordingly, the department believes that implementing a more comprehensive cybersecurity plan is a critical component of the initiative and a sound investment in the department's assets. The TIM project began in 2012 and is scheduled to conclude in 2019.

Analysis:

The department has already been working to improve, modernize and integrate its operations for several years. The department's efforts to bolster cybersecurity in the midst of escalating threats of cybersecurity incidents is core to protecting current and future investments in the TIM project made by the department, as well as safeguarding sensitive medical and financial data of more than 600,000 individuals.

The current request is a continuation of efforts that began during the 2011-13 biennium. The 2011-13 biennial budget, 2011 Wisconsin Act 32, set funding aside in the Committee's supplemental appropriation and allowed the department to request, without the finding of an emergency, additional expenditure authority and positions to address increasing workload and improve customer service. On September 14, 2011, the department received approval for supplements of $2,261,200 SEG in fiscal year 2011-12 and $1,572,400 SEG in fiscal year 2012-13.. On August 10, 2012, the department received an additional supplement of $2,702,500 SEG from the Committee for fiscal year 2012-13.

If a request for additional position authority is approved under Section 9112(1) of Act 20, the department is not required to request expenditure authority for compensation costs, as this funding is automatically supplemented. The department has once previously utilized the provisions of Sections 9112(1) and 9212(1) in Act 20. On May 20, 2014, the department received 4.0 FTE SEG permanent positions and 3.0 FTE SEG four-year project positions to provide support for the department's benefits administration and business process modernization project. However, the department used existing resources to fund these positions and did not receive supplemental funding for compensation costs in fiscal year 2013-14 or 2014-15. While it is unnecessary for the department to explicitly request additional expenditure authority associated with the positions, this request specifies the supplemental expenditure authority needed to pay compensation costs.

The department's cybersecurity initiative is not only an integral component of its modernization project, but has become especially critical as cyber risks and hacking crimes have escalated in frequency and severity. The federal government recently experienced the negative fallout of hacking incidents. Data breaches of the U.S. Office of Personnel Management and Internal Revenue Service exposed the sensitive, personally-identifiable information of millions of federal employees and taxpayers. The department cites a report from the Government Accountability Office, which outlines that federal agencies experienced more than 77,000 cybersecurity incidents in 2015 involving personally identifiable information, which is an increase of over 1,300 percent since 2006.

Similarly, state governments are not immune to the threats of hacking. In 2016, hackers targeted the voter registration systems in Arizona and Illinois, which led the Federal Bureau of Investigation to urge states to strengthen their cybersecurity efforts.

Furthermore, the department indicates that there are approximately 30,000 vulnerability scans and 2,000 brute force password hacking attempts each day on State of Wisconsin computers. The significant risks and consequences of cybersecurity breaches facing the department illustrate the importance of bolstering its cyberdefense functions.

The department has partnered with the Division of Enterprise Technology within the Department of Administration to develop a strategic cybersecurity plan. The division is responsible for safeguarding the core infrastructure of the state's technology assets, including servers and firewalls. The department is responsible for supporting and safeguarding its other, more customized technology assets. Since cybersecurity threats tend to be specifically targeted at specialized applications and sensitive data, it is preferable for the department, rather than the division, to implement a tailored cybersecurity program with security staff that has considerable knowledge of the department's technological infrastructure.

Currently, the department employs 1.0 FTE position and two contractors dedicated to performing cybersecurity responsibilities. In addition, the department has reallocated an existing position to create a chief information security officer, which will work closely with the requested positions. Approving the requested 3.0 FTE positions will ensure that the department will not have to reallocate resources from other benefits administration and modernization projects within the TIM initiative to these critical cybersecurity functions. Since the threats of cybersecurity breaches will continue after the conclusion of the TIM project, it is recommended that the department receive permanent position authority, rather than project positions, for this initiative. Findings and recommendations generated from annual third-party security audits will identify gaps in data security and will provide direction for the department's cybersecurity team.

Recommendation:

Approve the request. A multipronged, robust cybersecurity effort is not only integral to the department's business modernization initiative, but will also safeguard the sensitive, personally identifiable information of more than 600,000 people and shield the department from potential financial losses and the other negative consequences of a cybersecurity data breach.

Prepared by: Derek Sherwin
266-3382

STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

December 5, 2016

THE HONORABLE SCOTT WALKER
GOVERNOR OF WISCONSIN
115 EAST CAPITOL
MADISON, WI 53702

Dear Governor Walker:

The Department of Employee Trust Funds (ETF) is trusted with protecting detailed medical and financial records of more than 600,000 individuals. This type of personally identifiable information increases ETF's risk of being subject to a cyber-attack. As you noted at the recent Wisconsin Cyber Security Summit, Wisconsin is a leader in cybersecurity defense and protecting residents' health and financial information continues to be a top priority for the state. While ETF has taken steps to strengthen its information security posture, additional resources are necessary to properly manage the increasing risks.

Specifically, ETF requests the creation of 3.0 FTE SEG Computer and Internet Security Analyst permanent positions and $458,800 SEG in FY 2017 and $590,200 annual ongoing funding under s. 20.515 (1)(w), state operations appropriation, to implement and maintain a more robust cybersecurity program. The request includes $150,000 for cyber liability insurance and $130,000 for routine security audits annually. ETF has evaluated its cybersecurity strategy, governance, and practices as part of a risk assessment. Information gained from this analysis was used to develop a comprehensive cyber risk management strategy to mitigate risks of cyber threats. Additional positions are crucial to implementing this plan and protecting the medical and financial records of its more than 600,000 Wisconsin Retirement System (WRS) members, especially as ETF moves to managing all health and retirement benefits online.

The risks of underfunding cybersecurity defenses have never been greater. The frequency, complexity, and costs associated with attacks is increasing exponentially. By 2021, cybercrime is expected to cause roughly $6 trillion worth of annual damages, according to a newly published report authored by Cybersecurity Ventures and supported by security consulting giant The Herjavec Group. (Morgan, 2016) This represents twice the 2015 estimated $3 billion in damages experienced by governments, businesses and private citizens at the hands of cyber criminals. (Microsoft Secure Blog, 2016) The requested resources will allow ETF to continue to enhance our security posture by investing in new technologies, processes and capabilities in line with its strategic plan to manage cybersecurity risks.

Background of Request

2013 Wisconsin Act 20 (2013-15 Biennial Budget Bill) included non-statutory provisions that allow the Department to request the Governor to supplement any sum certain appropriation from the public employee trust fund or create or abolish positions that are funded from revenues deposited in the public employee trust fund for the purpose of modernizing business processes or integrating information technology systems of the Department (Section 9112 – Non-statutory provisions; Employee Trust Funds). The Joint Committee on Finance provided that ETF is able to utilize this passive review process until FY 2019.

ETF is in the middle of integrating its benefits administration systems and modernizing its business processes. The name of this enterprise-wide initiative or "portfolio" of projects is TIM, which stands for Transformation, Integration and Modernization. The goal of the TIM initiative is to implement modern, professional benefits administration technology along with business process improvements to more efficiently and effectively serve our members and participating employers. This multi-year effort will integrate 17 siloed and antiquated systems into a new benefits administration system (MyETF). Successful implementation will enable ETF to do the following: 1) meet the significant growth in demand for ETF services with limited need for additional staff; 2) meet the growing demand for online services; 3) increase operational efficiency; 4) achieve overall improvement in customer service; and 5) reduce long-term administrative costs for public employers throughout the state.

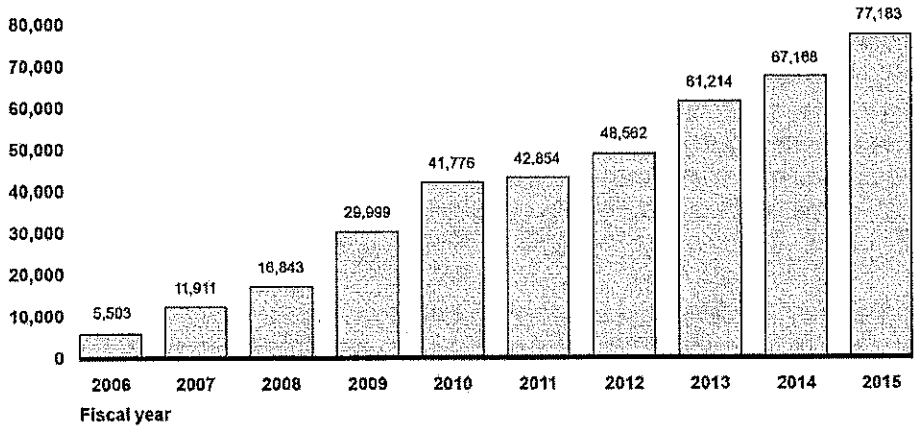
The TIM project, spanning from 2012 to 2019, will enable ETF to offer enhanced online member and employer services and maximize the capacity for handling an increasing number of annuitants. This major initiative is essential for the proper administration of the WRS and the other employee fringe benefit programs ETF administers. At the conclusion of this project, all business functions for members and employers will be available online. The resources requested are crucial to ensure that ETF advances its cybersecurity capabilities and remains a step ahead of cyber threats attempting to steal or compromise critical information.

Managing ETF's Cybersecurity Risks

Cyber Risks are Escalating

According to a fact sheet on the 'Cybersecurity National Action Plan' announced by the White House in February 2016, "Identity theft is now the fastest growing crime in America...Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year." Additionally, a report from the Government Accountability Office, noted that cybersecurity incidents in the federal government have skyrocketed by more than 1,000 percent in recent years. The report shows that in fiscal year 2015, federal agencies experienced 77,183 cybersecurity incidents involving personally identifiable information. The number of incidents has increased every year since fiscal year 2006, when that number was just 5,503. That's an upsurge of over 1,300 percent in just ten years.

TABLE 1. INCIDENTS REPORTED 2006-2014



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

As noted above, ETF manages medical or financial information for over 600,000 current or former employees and their beneficiaries or dependents. This information is often the most sensitive information for individuals. In relation to managing medical information, a new Ponemon Institute study highlighted that nearly 90% of all healthcare organizations suffered at least one data breach in the past two years with an average cost of $2.2 million per hack. The Ponemon report, commissioned by ID Experts, estimates that data breaches cost the healthcare industry about $6.2 billion. Additionally, 79% of healthcare organizations say they were hit with two or more data breaches in the past two years, and 45% had more than five breaches.

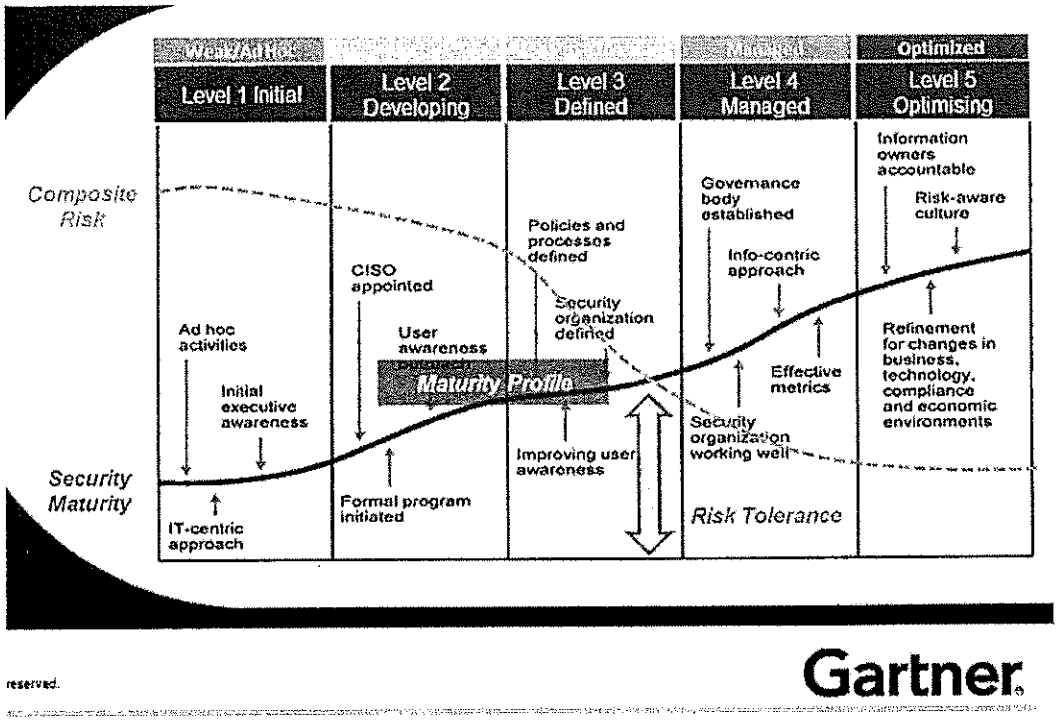
Wisconsin government is not immune. Every day, there are approximately 30,000 vulnerability scans on State of Wisconsin computer systems. There are also about 2,000 brute force attempts to crack State of Wisconsin passwords. The risks are very real.

Because of the programs ETF administers, ETF is required to retain member's financial and health data. ETF must protect this data. Given the increasing sophistication and severity of cyberattacks, ETF needs to continually improve its cyber defenses.

ETF's Current Cyber Security Process Maturity

The Department of Administration's Division of Enterprise Technology (DET) is using an information security diagnostic tool to assist in identifying security initiatives for the upcoming biennial budget. ETF is using the same tool to gain an understanding of its organization's current security risk. The tool allows an organization to develop a comprehensive understanding of information security maturity and make specific changes to improve its maturity. The Gartner maturity model shown in Table 2 rates organizations using five levels. ETF has launched a number of security initiatives designed to improve its information security maturity to an appropriately robust level.

Table 2. GARTNER INFORMATION SECURITY MODEL



reserved.

Gartner

ETF's Cybersecurity Roadmap

Development of enterprise risk management is crucial to addressing weaknesses and managing risks, faced both internally and externally. ETF created an enterprise Security Council to oversee and provide direction on ETF's security plan. The Council manages cybersecurity by using the National Institute of Standards and Technology (NIST) Cybersecurity Framework and integrating Center for Internet Security's Critical Security Controls.

The NIST framework provides a structure that organizations can use to create, guide, assess and improve comprehensive cybersecurity programs. The framework was designed to allow organizations – regardless of size, degree of cyber risks or cybersecurity sophistication – to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

The framework shapes an organization's cybersecurity program around five core functions, "identify, protect, detect, respond and recover." "Identify and protect" were the first steps in the early days of cybersecurity. These functions are still important, but "detect, respond and recover," have surged forward as a new focus in cybersecurity management. Additionally, ETF uses the Center for Internet Security's Critical Controls for Effective Cyber Defense (Controls), which was created to address the challenge of synthesizing all of the information in order to prioritize cybersecurity implementation. The Controls are a continually updated list of procedures, based on lessons learned

from actual attacks, and are designed to prevent, identify, address, and allay damage as a result of breaches.

ETF's security team recently identified 19 projects derived from the Controls that would enhance ETF's security today. Due to limited security staff resources, only a few of these projects have been completed. The requested positions will enable ETF to dedicate additional staff to security and provide the necessary resources to timely complete more of these important projects, while still maintaining focus on critical day-to-day security operations.

Part of ETF's cybersecurity plan is a strategic partnership with DET. DET supports the lower layers of the technology stack including networks, servers and other infrastructure, like firewalls. ETF is responsible for fully supporting its applications, platforms and middleware. Today's security threats are targeted at applications and the majority of current vulnerabilities are application and data-related. Successful cyber management involves knowing the organization to be protected. ETF staff are in the best position to do this.

The ETF Cybersecurity Roadmap allows ETF to improve its cybersecurity practices and work towards proactive threat mitigation. Staff in the new security positions will work on strengthening ETF's security and reaching the appropriate information security maturity level sooner.

Security Audits

ETF will continue to focus on strengthening its cybersecurity and broaden its use of technology to improve its business and financial procedures through Information Technology (IT) audits. This initiative will improve the maturity level in the Gartner security model by increasing its refinements for change in business, technology and compliance from continuous feedback from the audits. An IT audit is an assessment of an information system's security architecture and processes, as well as all related policies and procedures for managing data in a secure manner. IT audits can help organizations identify critical gaps in data security and reduce the threat of security compromises. This request provides annual funding authority for ETF to contract with a third-party expert in data security.

Cybersecurity Insurance

Cyber insurance is a risk transfer product that organizations can buy to mitigate losses due to IT problems. Gartner has defined cyber insurance as "protection against losses related to cyber risks, such as data theft/loss, business interruption caused by a computer malfunction or virus, and fines or lost income because of system downtime, network intrusion and/or information security breaches." The cyber insurance market, impelled by increasing costs due to loss of personally identifiable information, is estimated to be over $2 billion and growing.

Traditional commercial general liability and property insurance policies typically exclude cyber risks from their terms, leading to the emergence of cybersecurity insurance as a "stand alone" line of coverage. Cybersecurity insurance provides protection against a wide range of cyber incident losses that organizations may suffer directly or cause to

others, including costs arising from data destruction and/or theft, extortion demands, hacking, denial of service attacks, crisis management activity related to data breaches, and legal claims for defamation, fraud, and privacy violations.

ETF has been working with Risk Management professionals at DOA to perform a risk assessment and impact analysis to determine which type of cybersecurity insurance it needs. This has included a review of ETF's assets—including financial and customer data—as well as intellectual property. ETF also identified its main points of vulnerability during this process. DOA and ETF have engaged Aon, the State's contracted insurance broker, to obtain information and pricing on viable options.

The estimated annual cost of a policy appropriate for ETF's needs is about $150,000 annually. ETF's first line of defense is investment in a strong security program. Cyber insurance provides some secondary risk transfer for catastrophic losses. This will help advance ETF's maturity level in the Gartner arena by fostering a risk-aware culture that is continually looking to improve its security posture.

Security Positions – 3.0 Computer and Internet Security Analysts

Even as ETF's internal and Internet defenses improve, cyber criminals are persistent and patient when trying to exploit systems. Cybersecurity requires continual maintenance, analysis, research and optimization to stay up-to-date and to protect organizational resources from the latest threats and vulnerabilities. Gartner notes that processes must be in place to evaluate the need for applying patches and new configurations, and for ensuring that they are quickly and effectively rolled out. Currently, ETF employs one FTE and two contractors dedicated to performing all operational and project cybersecurity responsibilities. The work required to stay ahead of current threats exceeds ETF's existing resources and limits ETF's ability to improve, optimize and mature its cybersecurity practices.

Qualified staff are essential to detect cybersecurity threats against the agency. ETF security staff need to understand ETF's unique business operations and processes in order to identify and monitor unusual behavior in its networks. ETF has reallocated an existing position to create a Chief Information Security Officer (CISO) which will be responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO will direct staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology risks. The CISO responds to incidents, establishes appropriate standards and controls, manages security technologies, and directs the establishment and implementation of policies, procedures and appropriate training. The requested positions will work closely with the CISO.

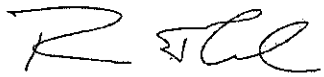
As noted above, ETF's security team is understaffed. Not having the necessary staff means that many important functions and projects are delayed. Providing ETF with three cybersecurity positions will help ensure that ETF is able to properly manage cyber risks and safeguard member's confidential information. The cybersecurity positions will primarily be responsible for implementing IT security activities; collaborating with DET on security management; maintaining and optimizing ETF's security alert software; improving vulnerability management processes; managing and improving ETF's

network security by working with DET to ensure that the firewalls are properly maintained; managing anti-malware software to protect all user workstations and legacy application servers; and routinely testing ETF's vulnerability (e.g., ethical hacking).

Conclusion

Cybercrime is rapidly evolving. Threats are now multi-layered, and growing increasingly sophisticated. As previously noted, the completion of ETF's TIM project will automate the administration of benefits for both employers and employees. This will provide better customer service, as well as increased efficiencies. This will also increase cyber-attack risks, which requires additional resources to properly manage these risks. The requested positions and resources are essential for ETF to protect confidential and valuable member information.

Sincerely,



Robert J. Conlin
Secretary

Cc: Waylon Hurlburt, State Budget Office

From:	Kraus, Jennifer - DOA
To:	Tappen, Gail A - DOA; Grinde, Kirsten - DOA
Cc:	Sherwin, Derek - DOA
Subject:	Fw: ETF Passive Review Request - Cybersecurity
Date:	Monday, December 05, 2016 7:46:23 PM
Attachments:	ETF Passive Review Request-Cybersecurity 12-5-16.pdf image002.png

---

Sent using OWA for iPhone

From: Hunter, Tarna - ETF
Sent: Monday, December 5, 2016 7:01:29 PM
To: Kraus, Jennifer - DOA; Sherwin, Derek - DOA
Cc: Henning, Pamela - ETF
Subject: ETF Passive Review Request - Cybersecurity

Hi Jenny and Derek,

Please find attached the Department of Employee Trust Fund's passive review request for the creation of 3.0 SEG positions in fiscal year 2017 and funding for cyber liability insurance and annual security audits. The requested resources will allow ETF to continue to enhance its security posture by investing in new technologies, processes and capabilities in line with its strategic plan to manage cybersecurity risks.

I look forward to working with you on this request.

Thanks,

Tarna

Tarna Hunter
Director of Strategic Engagement and Government Relations
Wisconsin Department of Employee Trust Funds
Ph. 608-267-0908

Sign up for ETF E-mail Updates – Look for the red envelope icon on our website.
Follow us on Twitter.

This email message and any attachments may contain information that is confidential, privileged, proprietary, or otherwise protected by law. This information is intended solely for the named addressee (or a person responsible for delivering it to the addressee). If you have received this message in error, please notify the sender immediately and delete it from your computer. Unauthorized disclosure, copying, printing, or distribution of this message is prohibited.