**14. POSITION SUMMARY**

This position serves as the Chief Information Security Officer (CISO) and Director of the Bureau of Information Security Management (BISM) under the general supervision of the Administrator of the Division of Management Services, and in close cooperation with ETF's Chief Information Officer (CIO). This position leads the agency in the development, adoption and use of strong security policies and measures to protect ETF's sensitive information, systems, and resources, while balancing this with the ease of staff and stakeholder access to sensitive information and the efficient use of computer systems. This position champions a risk-aware culture to help safeguard ETF information by applying people, processes, and technologies to minimize risk and foster security awareness. The CISO is a senior manager within the department, is a member of ETF's Agency Management Council (AMC) and operates under the governance of ETF's executive-level Strategic Council and provides quarterly updates to the Executive Team. This position also provides oversight and facilitation for ETF's Information Security Steering Committee (ISSC).

The CISO is responsible for ensuring that good information security practices permeate all aspects of ETF's business including our people, processes, technologies, and data. This includes tasks such as procuring and regularly assessing an appropriate cyber insurance policy, including security requirements in ETF department terms and conditions and vendor contracts, delivering routine security training for staff, reviewing departmental work procedures for security vulnerabilities, supporting IT security systems, testing and remediating the agency's information security defenses, developing and practicing incident response plans, and assessing and remediating unsecure staff behaviors. This position is expected to apply a risk management approach to identify, assess, and prioritize security risks and to minimize, monitor, and control the probability or impact of unforeseen events, using the appropriate and most effective security controls.

The CISO serves as the principal liaison with the Department of Administration's Division of Enterprise Technology (DET) Chief Information Security Officer and staff. Additionally, this position will lead the creation, upkeep, and testing of ETF's information security incident response plans. This position requires commitment to creating a diverse and inclusive work force.

**15. GOALS AND WORKER ACTIVITIES:**

40% GOAL A: Provision of guidance and oversight as ETF's Chief Information Security Officer (CISO)

Worker Activity

A1. Guide the agency while working within ETF's governance structure, in consultation with the Secretary's Office and in partnership with ETF's management, in the development, adoption and use of strong information security policies, measures, and controls to protect ETF's sensitive information, systems, and resources, while balancing this with the ease of staff and stakeholder access to information and business's efficient use of computer systems.

A2. Mature and grow information security as a valuable discipline that is vital to achieving the agency's mission and as everyone's responsibility through extensive communications, ongoing training, and sound organizational change management techniques.

A3. Prepare, implement, and maintain short-range and long-range information security plans, maintain strategic metrics, measure outcomes, and adjust plans as the cyber security landscape evolves.

A4. Develop, seek approval, socialize/market, and enforce information security and privacy policies that are consistent with agency program and administrative objectives, and in accordance with federal and state law via the ISSC, in collaboration with ETF's Policy, Privacy and Compliance (OPPC) Office Director, Office of Legal Services (OLS), CIO, HR Director, and others as needed,

A5. Update and train staff while working with management staff from across the department, on organizational strategies and work procedures that incorporate good security practices.

A6. Design, implement, and routinely practice comprehensive security incident response plans, and provide oversight for the remediation of security gaps and pain points.

A7. Maintain an excellent working partnership with DET, WI-ISAC, and other agencies. Represent departmental interests regarding state-wide information security standards, practices, and services provided by DET.

A8. Manage the preparation of annual, biennial and project security budgets; provide justification to acquire necessary resources, (personnel, software, and hardware) that best meet the information technology needs of the department.

A9. Advise the Secretary's Office and agency staff on how national and state-wide information security trends and incidents will impact the department and its programs. Provide perspective and recommendations to the OPPC Director or Office of Legal Services on the impact of new security laws and policies on operations.

A10. Educate and inform ETF's boards and staff on information security issues and challenges, and ETF's strategies for protecting the trust fund and its stakeholders' information.

A11. Coordinate, collaborate, and cooperate closely with ETF's CIO, CDO, information technology management, and staff.

A12. Use data-driven, quantitative and qualitative metrics on information security system administration, change efforts, incidents, vulnerabilities, etc. to measure, assess and inform the agency on risks and the resources needed to mitigate them, and to target security improvement efforts.

A13. Assess, consult, advise and initiate security-related improvements with vendors, technology consultants, and third-party program administrators.

A14. Audit routinely ETF's information security defenses, processes, systems, and staff behavior in conjunction with Director of the Office of Internal Audit and OPPC, utilize lean/six-sigma practices to maximize the value of security processes and defenses. Regularly contract for external security assessments. Respond to internal and external audit findings, implement recommendations or alternatives, or indicate contrary positions.

30% GOAL B: Provision of information security administration and project leadership and oversight

Worker Activity

B1. Evaluate and implement information security frameworks, such as ISO, NIST, and/or Gartner as a means of measuring, guiding, explaining, justifying, and promoting security initiatives.

B2. Provide for a current and continuing program of research and analysis in information security technologies and practices; and, for using the information gained in planning, developing and maintaining an effective security program.

B3. Set security system administration, implementation, and improvement priorities in coordination with departmental business and strategic plans.

B4. Provide effective project sponsorship, strategic guidance, team leadership, and project management oversight for information security improvement projects. Include regular review of: work plans and priorities, analysis, design, testing, implementation, written descriptive status reporting, post implementation evaluation, etc.

B5. Ensure staff understand and routinely follow computer system administration best practices, policies, and work procedures. This should be accomplished in close coordination and consistent with ETF's and DET's IT practices and standards.

B6. Understand and follow ETF's Internal Controls Plan. In partnership with the Information Technology Services Bureau, ensure that appropriate controls exist across the agency.

B7. Direct the establishment and maintenance of user communications and commitment through formal and informal techniques.

20% GOAL C: Management and supervision of Bureau staff

Worker Activity

C1. Comply with the ETF managerial standards at all times.

C2. Establish the Bureau organizational structure; organize and appoint standing or ad-hoc work groups, teams, and committees for purposes of communication, coordination, projects, and other special purposes.

C3. Staff the bureau and plan employee development through recruitment, selection, training, progressing work assignment, evaluation, promotion, retention, and career path training.

C4. Supervise bureau staff, including day-to-day activities and priorities, hiring, work assignments, performance evaluation, discipline, and resolving issues.

C5. Implement and administer appropriate department, division and bureau affirmation action goals, and health and safety. Assure principles are carried out in relation to hiring, training, reclassification, promotion and retention of employees; annual evaluation of supervisors and personnel.

10% GOAL D: Performance of special assignments, consultation, training, and/or support agency policy and participation in employee development programs

Worker Activity

D.1 Lead the development, upkeep, and testing of ETF's information security COOP/COG plans, in cooperation with the Agency's Continuity Manager,

D.2 Carry out special assignments to respond to the needs of agency management and the divisions.

D.3 Prepare special reports and recommendations as required.

D.4 Maintain a program of personnel development through appropriate training, selected reading, conferences, and seminars as attendee and participant.

D.5 Develop detailed knowledge of all Department internal and external administered programs to be able to proactively recognize potential security improvements and needed improvements in ease of access.

D.6 Attend schools, conferences, training sessions and workshops to increase and enhance job-related knowledge.

(Rev. 03/2021)

**Knowledge, Skills and Abilities Required**

1. Exceptional verbal and written communication skills, plus advanced interpersonal skills. Must be able to communicate and function as a trusted partner with ETF's boards, executives, management, and staff effectively, with poise, confidence, and clarity.
2. Exceptional presentation skills and ability to distill complex technical information into accurate, understandable terms to drive valuable discussion and decision making.
3. Ability to think critically, assess highly complex and technical options, and make recommendations.
4. Extensive knowledge of and experience leading the implementation and support of information security frameworks, work processes, computer technologies and policies.
5. Knowledge of and ability to apply modern management techniques.
6. Knowledge of strategic, business, information technology, and budgetary planning techniques for resource utilization, including feasibility and cost benefit analysis.
7. Knowledge of leadership, human relations, and other administrative and supervisory skills to develop effective working relationships with information security personnel.
8. Ability to use outcome-based data-driven metrics to measure the success and opportunities in ETF's information security efforts.
9. Knowledge of system administration methodology procedures, tools and standards, including documentation requirements and system testing techniques.
10. Knowledge of system hardware and software requirements used in a variety of modern business applications, including: data record keeping and retrieval, office automation, individual financial accounting, budgeting, general ledger accounting, procurement, human resources, general services, computer billings, statistical analyses and program results.
11. Knowledge of application development, database, network, desktop, mobile, web, etc. principals, work processes, methodologies, and technologies.
12. Knowledge of the uses and applications of financial, payroll, budget, accounting, case management, collaboration, knowledge management, and other software systems and tools.
13. Knowledge of IT and organizational change management techniques.
14. Knowledge of the department's mission, strategic plan, and goals.
15. Ability to employ traditional and iterative project management methodologies and techniques as appropriate.
16. Ability to provide project management sponsorship and oversight for complex IT and information security projects.
17. Knowledge of effective facilitation techniques.
18. Ability to work as a member of a team, as well as lead teams.
19. Knowledge of training development, delivery, evaluation methods and techniques.
20. Knowledge of Affirmative Action policies, employee health and Safety, employee assistance programs, and FMLA policies.
21. Ability to understand and promote the value of diversity, equity and inclusion in the workplace.