Position Summary:
This position develops and delivers a comprehensive information security and privacy program for the institution(s). Includes information in electronic, print, and other formats to assure that information created, acquired, or maintained by the university and its authorized users is used in accordance with its intended purpose to protect university information and its infrastructure from external or internal threats and to assure that campus complies with statutory and regulatory requirements regarding information access, security, and privacy.

Principal duties:
30% Leads the mission and vision of the university's cybersecurity operations.
- Develops and implements security risk and review, in addition to contractual oversight in security matters;
- Develops, plans, and implements long- and short-term campus security goals, projects, and initiatives;
- Exercises and demonstrates a holistic approach to cybersecurity risk mitigation across the university. Approach should include not only tools and technology, but consider factors such as human behavior, policies, incentives, risk transfer, and other practices that build and sustain a culture of secure and responsible use of information assets;
- Builds consensus, develops collegial, collaborative working relationships with stakeholders and peer groups.
- Partners with administrative and academic units (schools, colleges, divisions, and departments) to support initiatives, and gathers input from key stakeholders to support recommendations;
- Builds and maintains productive working relationships with campus partners.

20% Directs the UW-Madison Office of Cybersecurity (a department within the Division of Information Technology).
- Coordinates the enterprise development of information security policies, standards, and procedures in conjunction with IT leaders across the campus, Division of Information Technology, and University of Wisconsin System;
- Reviews process and coordinates reporting and response systems to address institutional information security, privacy, and copyright infringement incidents; Responds to alleged policy violations or complaints from external parties or internal reporting;
- Focuses departmental time and energy on proactive threat identification and champions mitigation strategies;
- Manages, develops, mentors, and supports a staff of cybersecurity professionals working in support of the university.

40% Serves as the institution's compliance officer with respect to the security components of the following obligations: Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, Digital Millennium Copyright Act (DMCA), Wisconsin Statutes, cybersecurity policy, USA Patriot Act, Payment Card Industry (PCI), and other relevant policies and regulations:
- Serves as the university contact for internal and external auditors and agencies, survey requests, and other relevant parties or requests regarding security/privacy matters;
- Collaborates with other units on campus that share compliance responsibilities for HIPAA, FERPA, Gramm-Leach-Bliley, DMCA, USA Patriot Act, PCI, Wisconsin Statutes, and other relevant policies and regulations.

5% Serves on various university review committees, working with a wide range of constituencies including the Faculty Senate, deans and associate deans, general counsel, and university leadership.

5% Advocates with University of Wisconsin System Administration for the cybersecurity needs of UW-Madison focused on the teaching, learning, and research missions of the university.