CISA ICR

Agency Information Collection Activities:

ReadySetCyber Initiative Questionnaire

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

CYBERFLORIDA.ORG

9 January 2024

CISA's Cyber Security Division's Vulnerability Management Sub-Division:

On behalf of the Florida Center for Cybersecurity, also known as Cyber Florida, I would like to thank you for the opportunity to submit a response to your information collection request and address the importance of securing the Nations critical infrastructure.

Cyber Florida was established by statute in 2014 to help position Florida as a national leader in cybersecurity by promoting cybersecurity education, research, and outreach. Hosted by the University of South Florida, Cyber Florida leads a spectrum of initiatives to inspire and educate future and current professionals, support industry-advancing research, and help people and organizations better understand and prepare for cyber threats.

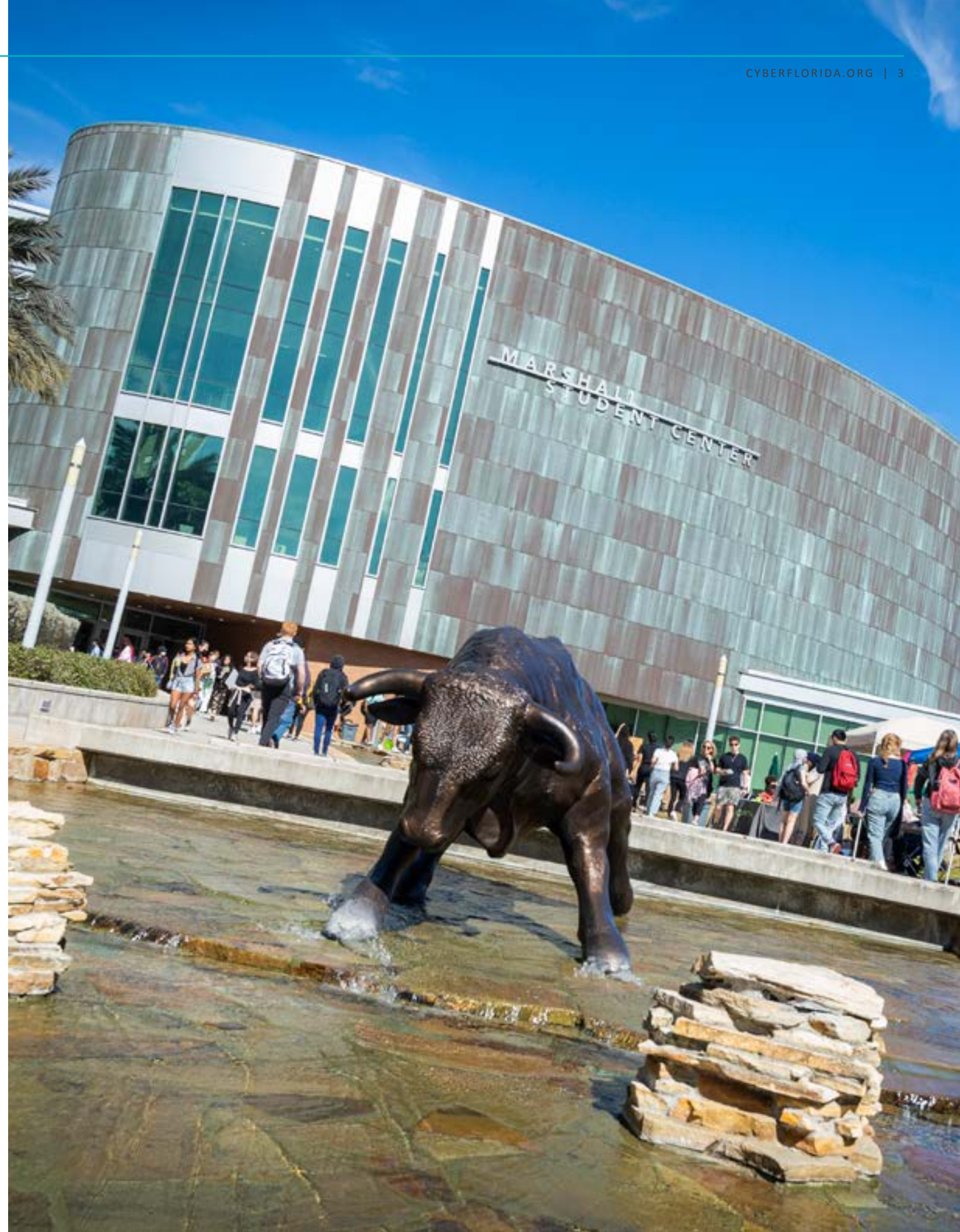
Among our key mission areas at Cyber Florida is to improve Florida's cyber readiness and we aim to do so through various assessment, education, and training initiatives. In this response, we provide an overview of our Critical Infrastructure Protection Program (CIPP), which directly aligns with the ReadySetCyber initiative, as the primary objective of the CIPP is to identify and mitigate systemic cyber risks that affect the safety, security, and privacy of Florida's critical infrastructure.

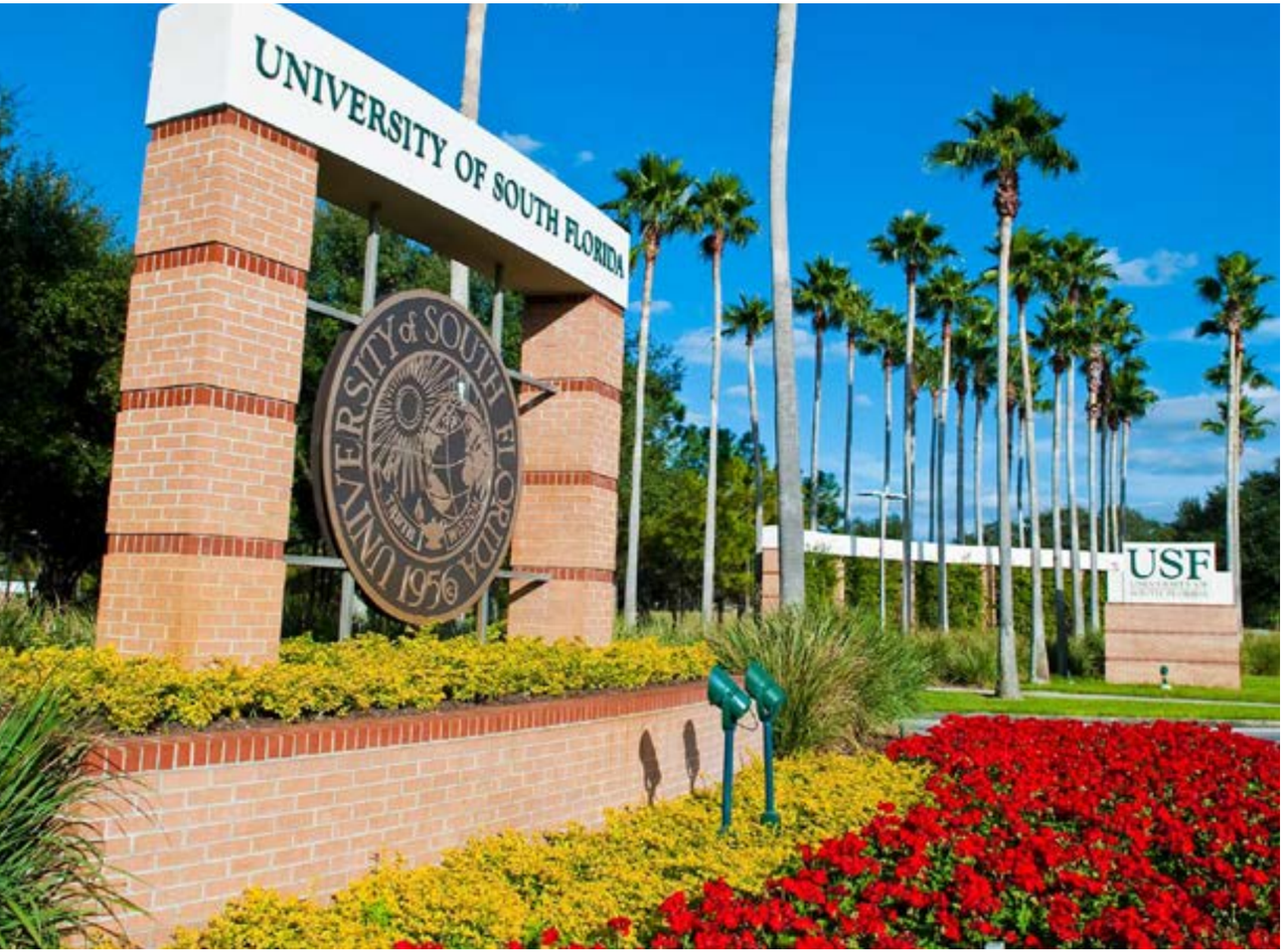
We commend the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget for leading the effort to secure United States critical infrastructure, as we believe this to be of utmost importance in our Nation's continuous fight against cyber threats. Cyber Florida is committed to serving as a resource to help CISA and OMB address this issue and others. We remain at your disposal for further discussion.

Respectfully,

General (Ret.) Kenneth F. McKenzie Jr.
Executive Director, The Florida Center for Cybersecurity

4202 E. Fowler Avenue, ISA7020, Tampa, FL 33620-7120 | info@cyberflorida.org | 813 974 2604





The Florida Center for Cybersecurity (Cyber Florida)

The Florida Center for Cybersecurity was established within the University of South Florida in 2014 under Florida statute 1004.444. The goals of the center are to: position Florida as a national leader in cybersecurity and its related workforce through education, research, and community engagement; assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce; act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training; seek out partnerships with major military installations to assist, when possible, in homeland cybersecurity defense initiatives; attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.

Critical Infrastructure Protection Program

In 2022, Cyber Florida was allocated $7M of non-recurring state funds from Specific Appropriation 2944B to complete a comprehensive cybersecurity "risk assessment for the state's critical infrastructure and provide recommendations to support actionable solutions for improvement of the state's preparedness and resilience to significant cybersecurity incidents"[1]. Cyber Florida partnered with Idaho National Laboratory (INL), a world leader in securing critical infrastructure (CI) systems, to customize their well-established and widely used cybersecurity evaluation tool (CSET) for the purpose of this statewide risk assessment. The online tool allows participants to identify cybersecurity strengths and weaknesses based on industry standards and to select appropriate security improvements from a database of cybersecurity standards, guidelines, and practices. Additionally, the CSET helps CI providers to prioritize cybersecurity improvements by identifying areas of greatest impact and/or vulnerability. To collect more nuanced, qualitative data, Cyber Florida worked with the MITRE Corporation, a leader in cybersecurity and national security consulting, to conduct a series of detailed interviews and guided discussions about the risks and challenges facing Florida's critical infrastructure providers. Furthermore, Cyber Florida conducted a broad, multi-modal campaign to raise awareness of the statewide risk assessment and recruit participants from the state's CI sectors. Outreach efforts included (but were not limited to) a branding/awareness campaign, ongoing outreach and consultation with all relevant state agencies and departments, a regional ambassador program, networking through sector-specific professional associations, an extensive email/direct outreach campaign, and networking/presentations at over 60 professional workshops/events.

The final report was submitted to the Florida legislature in June 2023 and included participation by more than 400 organizations representing 15 of the 16 critical infrastructure sectors. A subset of 230 organizations reached 90% or more completion of the assessment, yielding a representative data set. Based on key findings of the assessment and the recommendations provided to the Florida legislature, Cyber Florida has expanded the CIPP and has continued to collaborate with Florida's CI organizations, state and local agencies, sector-specific associations, and other stakeholders to identify and mitigate systemic cybersecurity risks. Through ongoing assessment, education, and training, our mission is to proactively and aggressively protect Florida's people, property, and prosperity from cyber victimization. With the expansion of the CIPP, participants are able to utilize various educational resources and training courses for executive, managerial, technical, and general staff that are tailored to the unique needs of the organization based on the areas of vulnerability identified in their individualized assessment results.

Comments

Guided by the NIST Cybersecurity Framework, Cyber Florida's critical infrastructure risk assessment primarily included cybersecurity-related yes or no questions, as well as demographic questions such as sector, subsector, customer base, and zip code of headquarters, totaling 156 questions in its entirety. To maintain anonymity and

[1] ***HB 5001: General Appropriations Act***

confidentiality, participants were not asked to provide a company name or physical address and the assessment is completed entirely online with no download required to participate. Upon completion of the assessment, respondents can save and print their unique set of reports to refer to while training staff and securing their systems. Based on our experience in conducting a statewide CI risk assessment, the questions included in the ReadySetCyber initiative appear to be relevant and will be useful in determining the cybersecurity needs of the organization.

Although the average time to complete the assessment of 156 questions is 90 minutes, through outreach efforts, we have discovered that many respondents have not been able to complete the assessment due to lack of time, unavailability of staff, and budget constraints. While the assessment is offered at no cost to the CI providers, we recognize that there is in fact an associated cost to participate in the form of time lost while completing the assessment, as many CI organizations are fiscally constrained and face significant staffing challenges. We quickly learned that providing more hands-on assistance to those completing the assessment greatly increased the number of respondents. Therefore, participants are able to contact Cyber Florida directly to speak with CSET experts who will walk them through the assessment until completion.

Further, we were faced with an additional burden of identifying the appropriate staffer to complete the assessment, as well as determining who is required to give permission for the organization to participate in the assessment. As such, we initially sought out CI organizational leadership to encourage participation and request permission, then identified specific IT/OT professionals within the organization to complete the assessment. As a result of our engagement and outreach efforts through the CIPP, we've been able to generate a statewide CI contact list (of over 8,000 contacts) that we intend to use for information sharing, widespread cybersecurity awareness and training resources, and cybersecurity emergency response purposes. Finally, despite our assurances regarding the safety and confidentiality of the information provided, many organizations chose not to complete the assessment due to concerns about data loss, data protection, data sharing, etc. Due to the voluntary nature of the assessment, we anticipate that we will not receive participation from all CI entities. However, we continue to encourage participation and advocate for the assessment due to the cruciality of the data and information produced, not only for critical infrastructure, but also for the state, as well as the remarkable resources that are available to CI providers based on individual results.

Conclusion

The critical infrastructure risk assessment that Cyber Florida conducted was, to our knowledge, the first of its kind across the nation. With many lessons learned, we've been able to effectively expand and enhance this program to allow for ease in participation and to encompass a convenient workflow that begins with assessing the significant cyber risks that may threaten an entity and ends with the specific education, training and resources that are needed to mitigate those risks. With the mission of creating a cyber secure and resilient state, we're proud to continue offering our Critical Infrastructure Protection Program. We commend CISA and OMB for their efforts in applying a similar model at the national level and are willing and eager to provide assistance if/where needed.

Contributing Authors

Jordan Deiuliis
Cyber Program and Policy Analyst
Cyber Florida: The Florida Center for Cybersecurity

Bryan Langley
Senior Executive Advisor
Cyber Florida: The Florida Center for Cybersecurity

Emilio Salabarria Sr.
Deputy Program Manager
Cyber Florida: The Florida Center for Cybersecurity

Contact Information

Ernie Ferraresso
eferraresso@cyberflorida.org
813 974 1869
Director
Cyber Florida: The Florida Center for Cybersecurity