Cybersecurity Leadership and Strategy 2-Day Comprehensive Training
FIU Jack D. Gordon Institute for Public Policy

Program Agenda

Program Opening – Day 1

Hour	*Session*
7:30-8:30	Breakfast
8:30-8:40	Welcome Program and Opening Remarks
8:40 - 8:45	Program Overview
8:45 -10:15	Module 1: Emerging Threats
10:15 - 10:30	Break
10:30– 12:00	Module 1.5: Emerging Threats Exercise
12:00 – 12:45	Lunch
12:45-2:15	Module 2: Organizational Cybersecurity
2:15-2:30	Break
2:30-4:00	Module 2.5: Organizational Cybersecurity Exercises

Program Continuation – Day 2

Hour	*Session*
7:30-8:30	Breakfast
8:30-8:40	Day 2 Program and Opening Remarks
8:40 - 8:45	Program Overview
8:45 -10:15	Module 3: Developing Cybersecurity Policy and Strategy
10:15 - 10:30	Break
10:30– 12:00	Module 3.5: Developing Cybersecurity Policy and Strategy Exercise
12:00 – 12:45	Lunch
12:45-2:15	Module 4: Implementing Cybersecurity Policies and Strategies
2:15-2:30	Break
2:30-4:00	Module 4.5: Implementing Cybersecurity Policies and Strategies Exercises

CYBER SECURE FLORIDA
This program is provided at no cost to Florida public sector employees through the CyberSecureFlorida initiative funded by the Florida Legislature and led by Cyber Florida.

Program Agenda

Cybersecurity Leadership and Strategy Professional Education Program

Program Overview:

The Cybersecurity Leadership and Strategy Professional Education Program is designed to arm elected officials, municipal and state leaders with essential skills in cybersecurity policy, strategy, and response. The program focuses on the requirements of the 2022 Local Government Cybersecurity Act, Florida Statute Section 282.3185.

Utilizing the NIST Cybersecurity Framework as a benchmark throughout its modules, the program ensures alignment with best cybersecurity practices. It's tailored to accommodate the varied leadership levels and contexts within local governments.

The program incorporates a series of experiential exercises and simulations, challenging participants to identify threats, formulate strategies, and respond to cyber-attacks in realistic scenarios, including those relevant to the 2022 Local Government Cybersecurity Act.

Participants will engage in group discussions, individual and team activities, and practical exercises to develop their understanding of cybersecurity principles. The program underscores the NIST Cybersecurity Framework as a key standard, equipping participants to implement this framework in their organizations for improved cybersecurity and compliance with legislative requirements.

Program Agenda

Cybersecurity Leadership and Strategy Professional Education Program

Module 1: Emerging Threats
This module focuses on understanding the current and emerging cyber threats facing the public and private sectors, examining the types of state and non-state actors perpetuating cyber threats, and assessing the challenges and opportunities in combating current and emerging cyber threats. A subsection addressing ransomware incidents, the primary focus of Florida Statute 282.3185, otherwise known as the Local Government Cybersecurity Act, is included.

Module 1: Emerging Threats
Learning Objectives

- Develop an understanding of the current and emerging cyber threats facing the public and private sectors: crime, information, intelligence, and cyber operations.
- Examine the types of state and non-state actors perpetuating cyber threats.
- Assess the challenges and opportunities in combating current and emerging cyber threats.

Module 2: Organizational Cybersecurity
This module develops an understanding of the interconnectedness of policy, operations, and technology while examining effective structures, authorities, and processes. Participants will assess the impact of policy on the private sector and how the private sector can support the government in countering cybersecurity threats. A subsection discussing the importance of timely reporting of cybersecurity incidents and ransomware attacks as mandated by Florida Statute 282.3185, otherwise known as the Local Government Cybersecurity Act has been included.

Module 2: Organizational Cybersecurity
Learning Objectives

- Develop an understanding of the interconnectedness of policy, operations, and technology.
- Examine the most effective structures, authorities, and processes as well as the risk considerations that should be taken into account.
- Assess the impact of policy on the private sector and how the private sector can support the government in countering cybersecurity threats.

Program Agenda

Module 3: Developing Cybersecurity Policy and Strategy

In this module, participants will learn the difference between policy and strategy, the key considerations for developing a cybersecurity strategy at the enterprise and national levels, and the fundamental building blocks for a sustainable cybersecurity framework. A subsection addressing the requirements outlined in Florida Statute Section 282.3185, otherwise known as the Local Government Cybersecurity Act, for creating and maintaining an incident response plan and providing employee training has been incorporated.

Module 3: Developing Strategies

Learning Objectives

- Develop an understanding of the difference between Policy and Strategy.
- Understand the key considerations for the development of a cybersecurity strategy at the enterprise and national levels.
- Establish fundamental building blocks for a sustainable cybersecurity framework at a national level using information sharing practices and processes.
- Understand assessment tools for developing a cybersecurity strategy.

Module 4: Implementing Cybersecurity Policies and Strategies

This module focuses on the challenges in implementing policies and strategies in both the public and private sectors. Participants will examine the keys to successful implementation of strategies to combat cyber threats and assess ways to measure effective implementation to safeguard national security and critical infrastructure. The course also incorporates material on the execution of the Florida Statute Section 282.3185, otherwise known as the Local Government Cybersecurity Act. This legislation includes specific mandates such as employee training and the annual reporting of cybersecurity incidents.

Module 4: Effective Implementation

Learning Objectives

- Develop an understanding of the challenges in implementing policies and strategies in both the public and private sectors, information sharing practices and processes.
- Examine the keys to successful implementation of strategies to combat cyber threats, have knowledge of the tools and resources available.
- Understand the importance and process of recovery following a cyber incident in line with the NIST Cybersecurity Framework and the Local Government Cybersecurity Act's specific requirements.