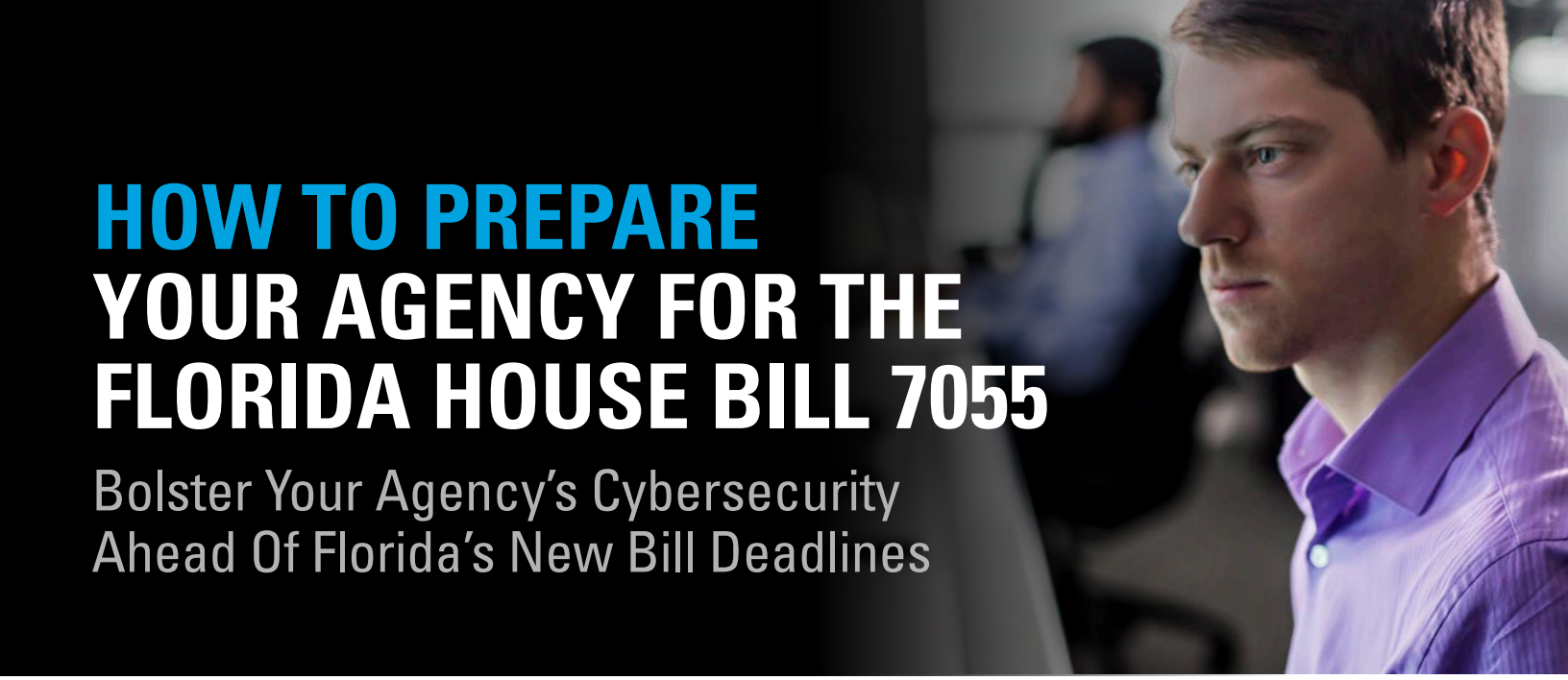


HOW TO PREPARE YOUR AGENCY FOR THE FLORIDA HOUSE BILL 7055

Bolster Your Agency's Cybersecurity Ahead Of Florida's New Bill Deadlines

Florida House Bill 7055 requires local governments to adopt cybersecurity standards that safeguard their data, information technology and information technology resources to ensure availability, confidentiality and integrity. The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology (NIST) and Technology Cybersecurity Framework. The next addendum requires local governments to report cybersecurity and ransomware incidents to the State Watch Office as soon as possible but no later than 48 hours after discovery for a cybersecurity incident and 12 hours after discovery for a ransomware incident. Finally, FLORIDA HOUSE BILL 7055 prohibits state agencies, counties, and municipalities from paying or otherwise complying with a ransom demand.

Overall, this new Bill includes a $67 million budget of nonrecurring state funding to assist local governments in complying with the provisions of the bill.

BILL HIGHLIGHTS

The state of Florida has introduced new cybersecurity measures that by 2025, will require your agency to:

- Establish a cybersecurity Incident Team/Plan & Report to FL COC and Cybercrime office ASAP
- Perform a Risk Assessment
- Will not be allowed to Pay or comply with any Ransomware demand Complete Cybersecurity Plan

AGENCY REQUIREMENTS & DATES TO NOTE:

Florida Counties:

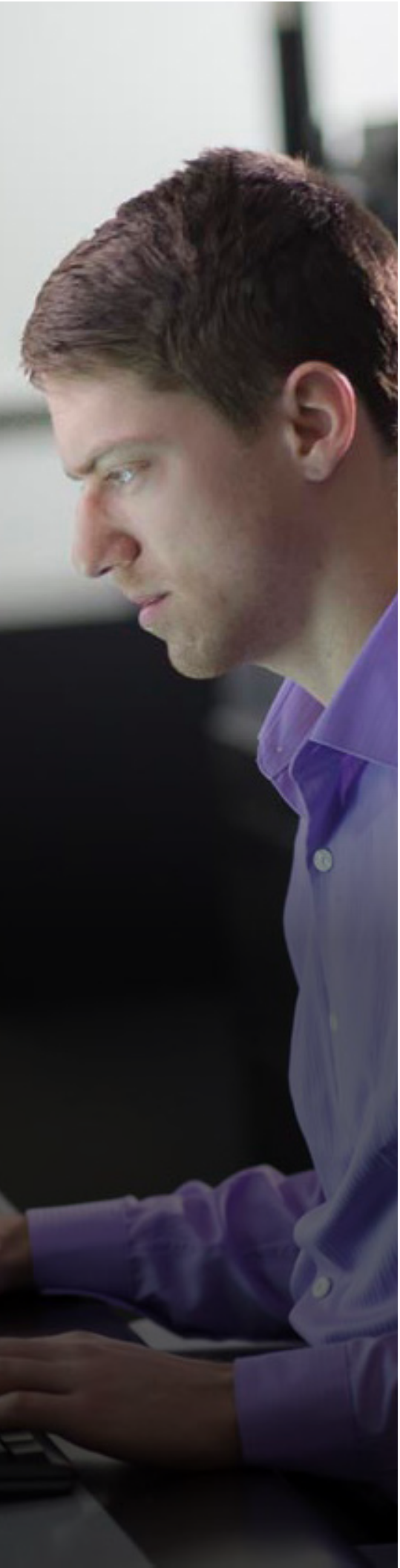
- Population > 75K adopt Cybersecurity Standards by Jan 1, 2024
- Population < 75K adopt Cybersecurity Standards by Jan 1, 2025

Florida Municipalities:

- Population > 25K adopt Cybersecurity Standards by Jan 1 2024
- Population < 25K adopt Cybersecurity Standards by Jan 1 2025

HOW MOTOROLA SOLUTIONS CAN HELP

- Incident Response Plan - Tested annually (Table top Exercises)
- Penetration Test - Annually or biannually
- Risk Assessment - Annually or biannually
- Bolster your Cybersecurity posture using tools to Monitor, Detect and Respond (MDR) to any threats in their environment.



CYBERSECURITY SERVICES TRUSTED SERVICE PROVIDER TO PUBLIC SAFETY

As a trusted business partner, Motorola Solutions Cybersecurity Services bring together an integrated portfolio aligned to the National Institute of Standards and Technology (NIST) framework to identify gaps in security programs, detect threats within networks, and prepare our customers for cybersecurity incidents.

MANAGED DETECTION AND RESPONSE (MDR)

Detect Threats like Ransomware in your networks and infrastructure.

- Identifies previously unknown threats without agent installation or impact on the network
- Identify previously unknown applications running on the network
- Alert on unknown attacks with flow anomaly detection

ADVISORY SERVICES AND CONSULTING

Identify gaps in your cybersecurity posture and prioritize weaknesses.

- Penetration Testing
- Risk Assessments
- Virtual CISO

INCIDENT RESPONSE PREPAREDNESS

Develop and test your organization's cyber incident response plan.

- Incident Response Planning
- Table Top Exercises
- Functional Drills

GOVERNANCE, RISK AND COMPLIANCE

Adhere to regulatory cybersecurity requirements in line with organizational needs

- CIS (Center for Internet Security)
- NIST (NIST CSF, NIST 800-53)
- FedRAMP

For more information about our Cybersecurity Services, contact your Motorola Solutions representative or visit **motorolasolutions.com/cybersecurity**

James Feild: +1-(443)-478-6995 / james.feild@motorolasolutions.com

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2022 Motorola Solutions, Inc. All rights reserved. 11-2022 [BB04]