Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

EMERGENCY DIRECTIVE 2025-05-01

Prohibited Offshore Resources, Personnel, Contractors

Date Issued: May 1, 2025

Table of Contents

Revision Control History

Version	Author(s)	Date	Description
1.0.0	Jason Silva	May 1, 2025	Initial Version

Approval

5/2/25

Jason Silva
Interim State Chief Information Security Officer

Date

Background

The Department of Information Technology (DoIT), Office of Security Management (OSM) is responsible for establishing security requirements for State information systems and information technology (IT) resources pursuant to Maryland Code, State Finance & Procurement ("SF&P") § 3.5-2A-04; and is headed by the State Chief Information Security Officer (CISO), in accordance with SF&P § 3.5-2A-03.

Pursuant to SF&P § 3.5-2A-04, OSM oversees the direction, coordination, and implementation of the overall cybersecurity strategy and policy for units of State government. OSM is also charged with developing and maintaining information technology security policy, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology (NIST).

The State CISO issues Maryland Cybersecurity Emergency Directives (ED) in accordance with the IT Security Manual. EDs are mandatory orders that require all units of the Executive Branch to take specific actions to address product, technology, resource or avenue of exploitation. EDs are issued in response to urgent situations that require immediate action to protect the organization, its assets, or its personnel.

Scope

This ED addresses all IT assets that generate, receive, store, process or transmit state data, whether the system is hosted on the State network or by a third-party provider.

The term **data** is defined as a subset of information in an electronic format that allows it to be retrieved or transmitted per NIST SP 1800-25B. **State Data** as defined by DoIT OSM is all data created or in any way originating with a Unit of State government, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, a service provider's hardware, or exists in any system owned, maintained or otherwise controlled by the State or by a service provider.

The term **unit of State government** has the meaning given in SF&P 3.5-101(f) ("an agency or unit of the Executive Branch of State government") *.*

The Maryland Data Classification Policy establishes the standards of information classification and outlines the security levels. Agencies are required to adhere to the Data Classification Policy and ensure the appropriate handling requirements in accordance with its data classification.

Effective Immediately All Offshore Operations Are Limited as Outlined Below:

1. Limited Operations

By order of the State CISO, all offshore operations activities will require a waiver at the State CISO's discretion . This directive applies to all units of State government utilizing current or new offshore resources directly or indirectly.

Offshore resources that require access to State Data and/or information systems present a moderate to high level of cybersecurity risk to the State. Below are a few examples of offshore resources that pose risks:

- Code Development
- Operations Staffing (call centers, maintenance, data processing)
- Systems or Applications

Offshore operations include processing data outside of the United States or its' territories to include operating or performing a set of operations on State Data, manually or by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2. Compliance Requirements

In order to comply with this ED, all units of State government that are currently utilizing offshore resources or will be utilizing new offshore resources, directly or indirectly, must submit the completed Vendor Risk Assessment Questionnaire Form: Offshore Resource Utilization form to OSM by emailing the Governance, Risk and Compliance (GRC) Team at doit.grc@maryland.gov. The following must be included in any request:

- Type of data being processed
- Define function of offshore resources
- Non-Disclosure Agreement (NDA) between State and contractor(s) and/or subcontractor(s)
- IT Security Manual controls applied
- Third-party and sub-contractor SOC 2 Type 2 reports
- Verification of contractors’ criminal background checks

All units of State government are required to comply with this ED. Any failure to immediately comply with this ED is considered a violation of State Cybersecurity policy and, per SF&P 3.5-2a-04(b)(6), may result in the State CISO determining, directing, or taking actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.

3. Communication and Reporting

Any anomalies, potential hazards, or emergency situations arising during any period of offshore resource engagement should, as in any such instance, be immediately communicated to the designated agency emergency response team per the unit of State government’s Incident Response Plan.