Report Highlights

Governor's Office of Information Technology
Judicial Branch

EVALUATION CONCERN

The Governor's Office of Information Technology and the Judicial Branch have technical security vulnerabilities that should be remediated. Additionally, there are areas for improvement on the governance side of information security.

KEY FACTS AND FINDINGS

- The **Governor's Office of Information Technology** (OIT) is responsible for oversight and governance of information security for all Executive Branch agencies.
- Our work identified 243 technical security vulnerabilities that should be remediated. Vulnerabilities are categorized according to nationally recognized Common Vulnerability Scoring System Version 2 (CVSS V2) methodology. The classifications in this system, from most severe to least severe are Urgent, Critical, High, Medium, Low, and Advisory.
    - We found zero Urgent vulnerabilities.
    - We found 27 Critical vulnerabilities.
    - We found 74 High vulnerabilities.
    - We found 142 Medium vulnerabilities.
    - We do not report on Low and Advisory vulnerabilities.
- Disaster recovery plans do not exist for the two critical enterprise applications we reviewed.
- We found areas for improvement of logical access controls.

- The **Judicial Branch** is responsible for oversight and governance of its own information security.
- Our work identified 9 technical security vulnerabilities that should be remediated.
    - We found zero Urgent vulnerabilities.
    - We found zero Critical vulnerabilities.
    - We found 3 High vulnerabilities.
    - We found 6 Medium vulnerabilities.
    - We do not report on Low and Advisory vulnerabilities.
- Disaster recovery plans do not exist for the one critical enterprise application we reviewed.
- We found areas for improvement of logical access controls.

BACKGROUND

Governor's Office of Information Technology:

- Was established in 2008.
- Centralized the management of Executive Branch information technology resources, including IT staff.
- Is responsible for securing networks, servers, databases, and web applications across Executive Branch agencies.

Judicial Branch:

- Manages its own IT services through the Judicial Business Integrated with Technology Services division.
- Is responsible for securing its own networks, hardware, databases, enterprise applications, and web applications.

KEY RECOMMENDATIONS

The Governor's Office of Information Technology should:

- Improve IT security by continuing the consolidation of IT services and processes, update policies, and train staff to follow prescribed policies.
- Work with business owners to develop, test, and update disaster recovery plans for the critical IT systems reviewed.
- Improve controls over logical access to critical IT systems reviewed.

The Judicial Branch should:

- Develop IT security policies in those areas that have a gap, including configuration and patch management.
- Develop, test, and update disaster recovery plans for the critical IT system reviewed.
- Improve controls over logical access to critical IT system reviewed.