AUTHORITY AND ADOPTION LETTERS
EXECUTIVE SIGNATORY PAGE
LETTER OF ADOPTION
RECORD OF APPROVAL
RECORD OF CHANGES
TABLE OF CONTENTS
1. INTRODUCTION
1.1 PURPOSE
1.2 SCOPE
1.2.1 Policy
1.2.2 Definitions
1.2.3 Relationship to Other Plans
2. SITUATION AND ASSUMPTIONS
2.1 SITUATION OVERVIEW
2.1.1 THREAT ANALYSIS
2.1.2 VULNERABILITY ANALYSIS
2.2 ASSUMPTIONS
3. CONCEPT OF OPERATIONS
3.1 PREPARATION
3.1.1 Preparation
3.2 DETECTION, ANALYSIS, AND NOTIFICATION
3.2.1 Impact Analysis
3.2.2 Notification and Activation Requirements
3.3 INCIDENT HANDLING
3.3.1 Containment
3.3.2 Eradication
3.3.3 Recovery
3.4 POST-INCIDENT ACTIVITY
4. ROLES AND RESPONSIBILITES
4.1 OFFICE OF ENTERPRISE TECHNOLOGY SERVICES (ETS)
4.1.1 Chief Information Security Officer (CISO)
4.1.2 Cybersecurity Team (CST) Responsibilities
4.1.2.1 RESPONSIBILITIES:
4.1.2.2 DURING A CYBER INCIDENT AFFECTING A STATE COMPUTER SYSTEM:
4.2 STATE DEPARTMENT OF DEFENSE
4.2.1 OFFICE OF HOMELAND SECURITY

4.2.1.1 THROUGH THE HSFC:
4.2.2 EMERGENCY MANAGEMENT AGENCY
4.2.3 NATIONAL GUARD
4.3 ATTORNEY GENERAL'S OFFICE
5. DIRECTION, CONTROL, AND COORDINATION
5.1 Reporting Requirements
5.2 Coordination
5.2.1 External Support
5.2.2 Federal Support
6. INFORMATION COLLECTION, ANALYSIS AND DISSEMINATION
6.1 Communications Response Process
6.1.1 Decide on team
6.1.2 Security alignment
6.1.3 Disclosure alignment
6.1.4 Stakeholder analysis
6.1.5 Selecting spokespeople
6.1.6 Present-day communications
6.1.7 Feedback loop
6.2 Activation of the Cyber Communications Response Team
6.3 Communications Coordination
7. PLAN DEVELOPMENT AND MAINTENANCE
8. AUTHORITIES AND REFERENCES
8.1 STATE LAWS, REGULATIONS AND DIRECTIVES
8.2 FEDERAL LAWS, REGULATIONS AND DIRECTIVES
8.3 REFERENCES
9. ATTACHMENTS
Attachment 1 – Acronyms
Attachment 2 – Checklist of major steps for Incident Response and Handling
Attachment 3 – Communications Tracking Worksheet
Attachment 4 – Compromise Questionnaire and Information Gathering
Attachment 5 – Cyber Incident Response Team Organization Chart
Attachment 6 – Cyber Incident Escalation and Workflow Diagram
Attachment 7 – Guidance on Reporting a Cyber Incident
Attachment 8 – Mission Area Activities
Attachment 9 – Sensitive Data Exposure Response Procedures
Attachment 10 – Threat Levels and Anticipated Response
Attachment 11 – Communications Checklists
Attachment 12 – Responsible, Accountable, Consulted, Informed (RACI) Matrix