

CYBER INCIDENT

RESPONSE & REPORTING PROGRAM (CIRRP) AMAZON WEB SERVICES (AWS)



amazon
web services

CIRRP

TABLE OF CONTENTS

Mission	1
Overview	1
Purpose	1
Scope	1
Roles and Responsibilities	2
AWS Shared Responsibility Model	2
<ul style="list-style-type: none">• Products• AWS Global Infrastructure• Customer Responsibilities	
Program	3
Incident Response Policy and Procedures	3
<ul style="list-style-type: none">• Distribution of Incident Response Policy and Procedures• Unauthorized Disclosure and Modification	
Cyber Incident Response and Reporting Program	3
<ul style="list-style-type: none">• The National Cybersecurity Protection Act of 2014 (NCPA)• Presidential Policy Directive (PPD) 41• Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure• Cybersecurity Discipline• National Cyber Incident Response Plan, October 2016, The Department of Homeland Security• Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1 National Institute of Standards and Technology January 10, 2017• Computer Incident Handling Guide, National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2.	
Core Capabilities	8
<ul style="list-style-type: none">• Core Capabilities Overview• Core Capabilities Matrix	
Data Matrices	9
<ul style="list-style-type: none">• Core Capabilities Matrix• Internal Incident Response Team (IRT) Personnel Matrix	

- Internal Incident Response Team (IRT) Incident Response Structure, Organization and Capabilities Matrix
- Amazon Incident Response Management Team Matrix
- Third-Party Incident Response Team (IRT) Personnel Matrix
- Third-Party Incident Response Team (IRT) Incident Response Structure, Organization and Capabilities Matrix
- Incident Response Training Matrix
- AWS Security Tools for Aiding Incident Response Matrix
- Internal Sources (i.e., Personnel) for Detection Matrix
- External Sources for Detection Matrix
- Risks, Threats, Attacks, and Related Incidents & Events Matrix
- Incident Response Notification Matrix (internal)
- Incident Response Notification Matrix (External)
- Notification (External) Critical Infrastructure Protection (CIP) Organizations Matrix

Team Structure 10

- Internal Incident Response Team (IRT) Personnel Matrix
- Internal Incident Response Team (IRT) Incident Response Structure, Organization and Capabilities Matrix
- Amazon Incident Response Management Team
- Third-Party Incident Response Team (IRT) Personnel Matrix
- Third-Party Incident Response Team (IRT) Incident Response Structure, Organization and Capabilities Matrix
- Assigned Titles and Respective Roles and Responsibilities
- Incident Response War Room

Incident Response Training 14

- Incident Response Training Matrix

Incident Response Testing 14

- Incident Response Testing – Coordination with Related Plans

Incident Response Preparation 15

- Incident Response Capabilities
- Incident Response Prevention

Incident Response Detection 17

- Precursors
- AWS Security Tools for Aiding Incident Response
- Internal Sources (i.e., Personnel) for Detection Matrix
- External Sources (i.e., Personnel) for Detection
- Information Spillage
- Risks, Threats, Attacks, and Related Incidents & Events

- Reportable Events
- List of Risks, Threats, Attacks, and Related Incidents & Events
- Risks, Threats, Attacks, and Related Incidents & Events Matrix

Incident Analysis and Response 23

- Technical Impact Analysis
- Business Impact Analysis
- Incident Rating Levels and Impact
- NCCIS Descriptions
- Documentation
- Notification (Internal)
- Incident Response Notification Matrix (Internal)
- Notification (External)
- Incident Response Notification Matrix (External)
- Notification (External) Critical Infrastructure Protection (CIP) Organizations
- Notification (External) Critical Infrastructure Protection (CIP) Organizations Matrix
- Notification (Insurance Carriers(s))

Containment, Eradication, and Recovery 28

- Coordination with Contingency Planning
- Evidence Collection and Investigation
- Incident Response Assistance
- Incident Response Assistance and Automated Support
- Automated Handling Processes
- Eradication
- Security Analysis & Recovery and Repair
- Communication

Post Incident Activities and Awareness 31

- Retention of Evidence

Incident Response Monitoring 32

- Automated Tracking, Data Collection, and Analysis
- Reporting of Suspected Incidents
- Coordination and Sharing
- Maturing Incident Response Capabilities

Glossary 35

Incident Response Submission Form (IRSF) 37