Information Technology and Cyber Security Services
Center for Response on Cybersecurity Incidents

RFC 2350 DESCRIPTION FOR CERT-GOV-MD CONSTITUENCY

1. ABOUT THIS DOCUMENT

CERT-GOV-MD constituents have a legitimate need and right to fully understand the policies and procedures of 'their' Computer Security Incident Response Team. One way to support this understanding is to supply, in conformity with RFC-2350, detailed information, which users may consider.

This document reflects and describes the set of key topics, which are in most concern and interest of the CERT-GOV-MD constituency.

1.1 Date of Last Update

This is version 2.2, published 12.08.2018

1.2 Distribution list for notifications

None available

1.3 Locations where this Document May Be Found

The latest version of this **RFC 2350** description document is available from the CERT-GOV-MD web site – www.cert-stisc.gov.md

Please make sure you are using the latest version.

2. CONTACT INFORMATION

2.1 Name of the Team

Center for Response on Cybersecurity Incidents CERT-GOV-MD

2.2 Address

Public Institution "Information Technology and Cyber Security Service"
Center for Response on Cybersecurity Incidents CERT-GOV-MD Republic of Moldova
Piaţa Marii Adunări Naţionale, 1
mun. Chişinău, MD-2012

2.3 Time Zone

GMT+0200, and GMT+0300 from April to October

2.4 Telephone Number

(+373 22) 820-900 (ask for the CERT-GOV-MD)

2.5 Facsimile Number

(+373 22) 250 522

2.6 Other Telecommunication

None available

2.7 Electronic Mail Address

For incidents: incidents@cert.gov.md
For other questions: info@cert.gov.md

2.8 Public Keys and Other Encryption Information

PGP key for info@cert.gov.md
User ID: Cyber Security Center CERT-GOV-MD <info@cert.gov.md>
KeyID: 0x8FB768E238D9FF60
Fingerprint: 7113 B2B6 ECD1 E297 FFD1 0D43 8FB7 68E2 38D9 FF60

PGP key for incidents@cert.gov.md
User ID: Center for Response on Cybersecurity Incidents (Incident Reporting PoC) <incidents@cert.gov.md>
KeyID: 0xB392CF67D9FF9E9C
Fingerprint: ED0A 3330 6139 B3F1 E204 32BF B392 CF67 D9FF 9E9C

2.9 Other Information

General information about the CERT-GOV-MD, as well as links to various recommended security resources, can be found at www.cert-stisc.gov.md

2.10 Points of Customer Contact

Secretariat
Telephone: (+373 22) 820-900
Fax: (+373 22) 250-522
E-mail: stisc@stisc.gov.md

Info CERT-GOV-MD
Telephone: (+373 22) 820 – 921
E-mail: info@cert.gov.md
PGP Key**:** 0x8FB768E238D9FF60

Incident Reporting Point of Contact
Incidents: incidents@cert.gov.md
PGP Key: 0xB392CF67D9FF9E9C

Press Relations
Telephone: (+373 22) 820-900
Designated person:

CERT-GOV-MD's hours of operation
08:00-17:00 Monday to Friday except official holidays

3. CHARTER

3.1 Mission Statement

CERT-GOV-MD is a team of cybersecurity experts, whose main task is to respond to the incidents related to information systems. The Center assists beneficiaries of information and telecommunication systems of public administration authorities in implementation of proactive and reactive measures in reduction of IT security risks and in assistance in incident response.

The goals of the CERT-GOV-MD are:

- Improve the level of cyber security within the government and increase confidence in new technologies;
- Reducing damage caused by security incidents;
- Raising the awareness of public authorities and government institutions through information, awareness and continuous training;
- Building strategic relationships to improve cyber security;
- Sharing information and lessons learned.

3.2 Constituency

CERT-GOV-MD's constituency are central and regional state governance authorities, specialized organs of state security and telecommunications, academies and universities of the Republic of Moldova as defined in the Government Decision № 840 of 26.07.2004 and its Annex №1.

Internet domain and/or IP address information describing the constituency: AS25319 and AS39279

3.3 Sponsorship and/or Affiliation

“Information Technology and Cyber Security Service” (“ITSec”) is a public institution subordinated to the Government of the Republic of Moldova (Government decision No. 414 of 08.05.2018) responsible for administration and maintenance of state information systems and infrastructure, telecommunication system of public administration authorities, for ensuring cybersecurity, for governance of unified state infrastructure of public keys as well as for implementation of information technologies in the public sector. The organization hosts

governmental computer security incident response team "Centre for Response on Cybersecurity Incidents CERT-GOV-MD" as an internal department within its organizational structure. https://stisc.gov.md/

3.4 Authority

The CERT-GOV-MD authority spans on informational and telecommunication systems of public administration authorities (AS25319 and AS39279) and is limited by the role of its sponsoring organization Public Institution "Information Technology and Cyber Security Service".

4. POLICIES

4.1 Types of incidents and level of support

The CERT-GOV-MD is authorized to address all types of computer security incidents, which occur, or threaten to occur in Moldavian informational and telecommunication systems of public administration authorities of "Information Technology and Cyber Security Service".

The level of support:

- coordination of actions in case of cyber incidents;
- advice about finding a response solution;
- advice to implement proactive measures in scope of preventing these security incidents occurring.

4.2 Co-operation, interaction and disclosure of information

CERT-GOV-MD exchanges all necessary information with other CSIRTs if they are CERT-GOV-MD partners in investigation of a security incident, only if all necessary measures were taken in order to prevent any form of identity disclosure, and, if this is not possible, only if CERT-GOV-MD is explicitly authorized by affected party.

All sensitive data and information are transmitted in encrypted form.

4.3 Communication and authentication

In view of the types of information that the CERT-GOV-MD will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

5. SERVICES

CERT-GOV-MD assists beneficiaries of information and telecommunication systems of public administration authorities in implementation of proactive and reactive measures in reduction of IT security risks and in assistance in incident response through providing a set of services.

The basic services of CERT-GOV-MD are:

- Alerts and warnings
- Artifact response
- Artifact response coordination
- Incident analysis
- Incident response support
- Incident response coordination
- Vulnerability analysis
- Vulnerability response
- Vulnerability response coordination
- Intrusion detection services
- Security-related information dissemination
- Awareness building

6. INCIDENT REPORTING FORMS

The current version of incident report form is available at www.cert-stisc.gov.md

7. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-GOV-MD assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.