RFC 2350 BPS-CSIRT

1. Document Information

This document contains a description of the BPS-CSIRT based on RFC 2350, which is basic information about the BPS-CSIRT, explaining responsibilities, services provided, and how to contact the BPS-CSIRT.

1.1. Last Update

The current version is 1.0 and issued on October 01, 2021.

1.2. Distribution List for Notifications

There is no distribution list for document update notifications.

1.3. Location Where This Document May Be Found

This document is available at
https://csirt.bps.go.id/assets/rfc2350/rfc2350-id.pdf (Indonesian)
https://csirt.bps.go.id/assets/rfc2350/rfc2350-en.pdf (English)

1.4. Document Authenticity

Both documents have been signed with BPS-CSIRT's PGP Key. For more details can be seen in Section 2.8.

1.5 Document Indentification

Documents have attributes, that is:

Title	: RFC 2350 BPS-CSIRT;
Version	: 1.0;
Publication Date	: October 01, 2021;
Expired	: This document is valid until the latest document is published.

2. Contact Information

2.1. Team Name

Badan Pusat Statistik - Computer Security Incident Response Team
Shortname : BPS - CSIRT.

2.2. Address

Badan Pusat Statistik
Jl. Dr. Sutomo 6-8 Jakarta

2.3. Time Zone

Jakarta (GMT+07:00)

2.4. Telephone Number

(021) 3519746

2.5. Fax Number

-

2.6. Other Telecommunications

(021) 3841195, (021) 3842508, (021) 3810291 Ext 3320

2.7. E-Mail

csirt[at]bps.go.id

2.8. Public Keys and Data Encryption

PGP *key* file is available at :
https://csirt.bps.go.id/assets/bps-csirt.asc

2.9. Team Members

The head of BPS-CSIRT is the Director of the Statistical Information System. Team members include Functional Officers at the Directorate of Statistical Information Systems.

2.10. Other Inormation

None available.

2.11. Points of Customer Contact

The recommended method for contacting BPS-CSIRT is via e-mail at the address csirt[at]bps[dot]go[dot]id or via telephone number (021) 3519746 on weekdays at 08.00 - 16.00.

3. About Gov-CSIRT

3.1. Vision

The realization of cyber security in supporting quality IT services for BPS, in realizing Advanced Indonesia

3.2. Mision

The mission of BPS-CSIRT are:
1. Carry out cyber security activities for IT services.
2. Increase the capacity of resources in the aspects of prevention, response and recovery of cyber security incidents.
3. Build awareness of cybersecurity threats among IT service users

3.3. Constituency

BPS-CSIRT constituents are users of IT services within the BPS

3.4. Sponsorship and/or Affiliation

BPS-CSIRT is part of the Directorate of Statistical Information Systems so that all funding comes from the APBN.

3.5. Authority

BPS-CSIRT has the authority with its constituents in handling cyber security disturbances. BPS-CSIRT can coordinate and cooperate with other competent parties for incidents that cannot be handled.

4. Policies

4.1. Type of Incidents and Level of Support

BPS-CSIRT serves the following types of cyber incident handling:

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phising;
e. Spamming.

The support provided by BPS-CSIRT to constituents may vary depending on the type and impact of the incident. Incident handling services based on constituent reports.

4.2. Cooperations, Interaction and Dislocure of Information

BPS-CSIRT will collaborate and share information with CSIRT or other organizations in the scope of cyber security. All information received by BPS-CSIRT will be kept confidential.

4.3. Communications and Authentication

For normal communication, BPS-CSIRT can use email without data encryption (conventional email) and telephone. However, for communications containing sensitive/restricted/confidential information, you can use PGP encryption on email.

5. Services

5.1. Main Service

The main services of BPS-CSIRT are:

5.1.1. **Warning Regarding Cyber Security**
This service is in the form of providing warnings of cyber incidents to owners of electronic systems and information related to services.

5.1.2. Cyber Incident Handling

This service is in the form of coordination, analysis, technical recommendations, and on-site assistance in the context of cyber incident response and recovery.

5.2. Additional Services

The additional services of BPS-CSIRT are:

5.2.1. Handling Electronic System Vulnerabilities

This service is in the form of coordination, analysis, and technical recommendations in order to strengthen security (hardening).

5.2.2. Digital Artifact Handling

This service is in the form of handling artifacts in the context of recovering affected electronic systems or supporting investigations.

5.2.3. Notification of Observation Results of Potential Threats

Notification of observations related to potential new threats that may occur.

5.2.4. Attack Detection

Detect various attacks that occur and are monitored through a security detection and monitoring system

5.2.5. Cybersecurity Risk Analysis

This service is in the form of identification of vulnerabilities and risk assessment of vulnerabilities found. Furthermore, recommendations are given that can be done to reduce these risks.

5.2.6. Consultation Regarding Cyber Incident Preparedness

Providing consultation related to cybersecurity incident response and recovery preparedness.

5.2.7. Building Awareness and Concern for Cybersecurity

Socialization and guidance to all employees within BPS, which aims to increase employee awareness and concern about cybersecurity.

6. Incident Reporting

Reports can be sent via email csirt[at]bps[dot]go[dot]id or through the website csirt.bps.go.id by attaching: logfile, timestamp, screenshot, name of the reporter, telephone number.

7. *Disclaimers*

- Until now, BPS - CSIRT has only responded and handled cyber security incidents that occurred on official work equipment;
- Regarding the handling of incidents of malware types depending on the availability of the tools they have.