# RFC 2350 Gov-CSIRT Indonesia

## 1. Document Information

This document contains a description of Gov-CSIRT Indonesia in according to RFC 2350. It provides basic information about the Gov-CSIRT Indonesia, its channels of communication, and its roles and responsibilities.

### 1.1. Date of Last Update

The current version is 1.0 and published on December 20, 2018.

### 1.2. Distribution List for Notifications

There is no distribution list for notifications.

### 1.3. Locations where this Document May Be Found

The current version of this document can always be found at
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-id.pdf (bahasa version)
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-en.pdf (english version)

### 1.4. Authenticating this Document

Both documents have been signed with the PGP Key of Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) - Badan Siber dan Sandi Negara (BSSN). See section 2.8 for more details.

### 1.5. Document Identification

Both documents share the same attributes
Title           : RFC 2350 Gov-CSIRT Indonesia
Version         : 1.0
Document Date   : December 20, 2018
Expiration      : This document is valid until superseded by a later version

## 2. Contact Information

### 2.1. Name of the Team

Government - Computer Security Incident Response Team (CSIRT) Indonesia
Short name: Gov-CSIRT Indonesia

### 2.2. Address

BSSN
Harsono RM 70
Ragunan – 12550,
Pasar Minggu, South Jakarta
Indonesia

### 2.3. Time Zone

Jakarta (GMT+07:00)

## 2.4. Telephone Number

+6221 78833610

## 2.5. Faximile Number

None Available

## 2.6. Other Telecommunication

None Available

## 2.7. Electronic Mail Address

bantuan70[at]bssn.go.id

## 2.8. Public Keys and Encryption Information

Bits            : 4096
ID              : 0x73802BD6
Key Fingerprint : 1A35 DAEF E63B BE93 C314 3272 CE5D 2119 7380 2BD6

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBFtex4QBEADfLdjiJbwGTgOXUwyt/emyua3wIfYufUgpAKAzk2Dz8t9aj5bt
Co3adcXQw+5WnKSHbD7Q2VFUgLd+whIVuf6rAUraMcMrR10xWvvq2x4kEIEQiBXQ
CZOLgbN/9n+u2GqcD3x/XimyUDSN+I7DGh8+CioTWcahRQfcX70AqTlw5+VNFHT6
mrwAYfH8aQN2aPG+vW7j5K3AIEHVYFLYnU8F0FqBpcyFFlAWhqRgp6Jscsn9w0Ty
dR/v8laoaX1iE35XVyX3TXjS8TH+DCBuSP3BV0LVJJyISoEO4X0plKmERGW5UzaQ
CEbawtopt73QgWKcO5DTgMI247X3kekMchU8ENf25LdzrZ8znw8+DH/PggcCu6Hh
R/bccgXoFhQbrieZbDtuXKYn22/jJMWDKpJMQkGsPV2+qlMdYOXRrU87MhBE4dk2
dXLYCJki2qYnwddZp0HxRn6zznQ2VIrF+N3cBnQQB8izBFqcgy6gvkmJiUrGRn9n
upRryX7Wp1djfA13Veb1HftQNauOcWsJQt//fj5+MC9P6r3A4S2rgnojQv3zuPxP
XUVuvZOE0ywqXTfxPd7DdJE3ilP8fLvdWEZoFHIZkBkAZtFFsbjNlEhUc7lBQtOR
B7wRptGQxajH26ru/atRpcfxAFx6pfYG5Hr0X1a7xqmpvPdxFcs5dQ0NnwARAQAB
tDRCYW50dWFuNzAgUHVzb3Bza2a2Ftc2luYXMgQINTTiA8YmFudHVhbjcwQGJzc24u
Z28uaWQ+iQJUBBMBCAA+FiEEGjXa7+Y7vpPDFDJyzl0hGXOAK9YFAltex4QCGyMF
CQlmAYAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQzl0hGXOAK9Y9lA/+NULC
uXxF+Ko/l3x482/7yJS6oElhqY17nskNFjmBqM6fwTFdQybarqs1AgxN3ne26MWs
VcmhSLsOaiN7tEnD0jPIRgqCZ4SnXeqthbuIoCb6cMI4Mae1gRRM4pb1ec4OyriW
infNAa+zWolZNuQG0cz/xuVme34Imv3Nv9WutCuyjGR3Renixlg68Sww7tV4x3gw
bkqu/3HReG9t39maeDafw6w0//oHyAqPA8vk36sK9Pt0zjro/q8s8W3NzsHnh/Ca
HX40WsX7oZPGBm0ILdHxwCXhhXmBY/aYBsSIC4AvYLrHRTHFCWxk6B6pL8rte06b
xyzICVQmQJLfn/QF9OhttIpYTY02yppGRRs9Tvyf+xTfZyIMoKeDjJmymZ1D421B
BguRR+zaxdrQwza1B3RlQ+8VKG/Mjf/zmnRAxSssXLm4LJ/KtpFWhI1lUDMhaMc8
fFOxH3Oj+N+tAPvM34LN1EJrDR/r6AggwBciM5ak1gtijlJS85NLFWHbFhQwHdZM
3kiTYNgYJ2uvfq7enswzMk/jy2bjd17UVTzfxpg3gz0iZ52hBnHl8DEtw4l5KQgS
ys4Nmen51ZyIyT+NfD73vk3nS41cI36d4YV97FlQ7rbaitNVFFBKV5fVSfkFrwKW
akU0T8oeCOiNuwLQWXdg3447BLyhNObQWL3YoKq5Ag0EW17HhAEQALwqDRRG5byw
MDLVQTTWdqeK5cezTKw5Ebj50tk0VSTaG3hDfwkwyPJjzTkuwPUEQb+6mEtOqQ2P
x9jIQylumI0Uy3NBd5wkaS9ZxEa9HU70VXeDIvAx+0eJeVNMCUcdgU28/nCnzAIr
3+5lseTg4MRrSo9xfgqYFd+QE5wmYGRO7/gXhvMf9vrVr8lcIvWWxYKUGl0bYoct
5ZSepTZ2mDJoJoOeuoTMW0WOfbGHzs1jS950PqqXri+n9LzupYc2FF3NEBRw1NuLY
MnwwDkqbGeLSnFEaOXce8BD9Ppnh1CK0dMwTWBCUIAUJXRNWRMN5prREs8gVRkJ0
GuRaMmji+lJHg5HfuXV3zKWJ3UBnCM1MpIpvFReMH2OPHWzeObAXcpg6OsPCk+99
MLjmkC/C2cZtHf48JJCRMtrTUN0165DJFXoJcCinaNRUx+YnHVTC5Wuu4+DVaCzY

5WbNc6LaQkA1PMK9oqBXFDtERXirbacw4kOpvoC+J0B6xnYDrAOQ8cAc9pSO7QSf
Y0NZYhDoJz6o5++TSt6P8Ol/LdsVFIK0TLhf1qiqMhuibCQi6Fom7r6D5wtuZ+22
Mn2Jw8nuMYvo7ze3p5jwoErCpPswh6AqSia8kTgMUoDNPJwuoC7m0dzWvQ99reNr
K9QdhjC3LtclPQolqibVz/Hfm3trciGlABEBAAGJAjwEGAEIACYWIQQaNdrv5ju+
k8MUMnLOXSEZc4Ar1gUCW17HhAIbDAUJCWYBgAAKCRDOXSEZc4Ar1jzKEACI7rht
7nF1cYEZpbwU3u8MTZXSCxu/kgmxYmJlnQhRhahwtWf5N/xn0lJtMGoic5wbpAvu
JqE/5OOTyd3dUx5eOtBjaEFf5Zw1Ar96K9x764YtJIyiq2WYuMK2EEYX8uoqpGCu
9iGqnis1EWOca5cSzjo60McN+UoMSTltja8XgLOAVkIxcz9CepRucBf/yugc6ENT
eUcA6Dv84tO4f0E5aKuXxk7ESMk/Whukz2PCsSaqs5K+1yCAZvU2aio4XYr2GJr9
VpI++A57r7lJqrhdIUJjuJmLGdV1HOTl3lTWkXi4XhNbsgeAjZ9iU3wjl1kSwf3P
aunf2wLww+j9sTuIaIZ6UWpnLCRbsA8IkVtFFczuM4NrBktFKx5y1QmdfTHgsmCS
8McEOEOZyGLngRWUwuhrKQI7okrxXhbQGMlNdSQ1IuPw0Bx7aYsUWnEFqMOApLAB
2Zm7CqYfrwsNGp6sWAwimO+05AOvr7jcqeBfwYyfDImO0Rf75YjPU6yJ+4NyEUWE
JubnHIYk47fV4T6O7BjvdgHIYHe51qDKo6xxmt32Wcn05fzGxTaPclgBC3krrwNB
vkPTTMDlkJ6fEBe5q476Xs+7RPRmlr4FE5tu7/GoVGKJCKIvXJWCZrYawhACjE8h
WGksMO/XgZgXAA1/KIljfJUJ0rjPMjgktq23Zg==
=yC+0
-----END PGP PUBLIC KEY BLOCK-----

The PGP key file can always be found at
https://bssn.go.id/wp-content/uploads/2018/08/Publik-Key-Bantuan70-pub.asc

## 2.9. Team Members

The Acting Head of the Gov-CSIRT Indonesia is the Director of Response and Recovery for the Government Sector of BSSN. The team members include all BSSN staffs in the government sector.

## 2.10. Other Information

None available

## 2.11. Points of Customer Contact

The preferred method to contact Gov-CSIRT Indonesia is to send an e-mail to Pusopskamsinas at bantuan70[at]bssn.go.id or call +6221 78833610 which is active 24/7.

## 3. About GovCSIRT

### 3.1. Mission Statement

The missions of the Gov-CSIRT Indonesia are:
a. to build, to coordinate, to collaborate, and to operationalize the government sector cyber security incident mitigation system, crisis management, and response and recovery
b. to establish cooperation in the context of response and recovery of cyber security incident that occurred in the government sector
c. to develop the government sector cyber security incident response and recovery resource capacity
d. to encourage the establishment of the government sector CSIRT

### 3.2. Constituency

The constituencies of the Gov-CSIRT Indonesia include central government, and region I and II local government namely:

a. The Central Government is the President of the Republic of Indonesia who holds the power of the government of the Republic of Indonesia which is assisted by the Vice President and the Ministries as referred to in the 1945 Constitution of the Republic of Indonesia

b. The Regional Government of Region I is the Provincial Government which covers the area of Aceh Province, North Sumatra, Riau, West Sumatra, Riau Islands, Jambi, South Sumatra, Bangka Belitung, Bengkulu, Lampung, Special Capital Region of Jakarta, West Java, Banten, Central Java, Special Region of Yogyakarta, East Java, and Bali

c. The Regional Government of Region II is the Provincial Government which covers the provinces of West Kalimantan, Central Kalimantan, South Kalimantan, East Kalimantan, North Kalimantan, North Sulawesi, Gorontalo, Southeast Sulawesi, Central Sulawesi, South Sulawesi, West Sulawesi, East Nusa Tenggara, Nusa Tenggara West, West Papua, Papua, Maluku and North Maluku

### 3.3. Sponsorship and/or Affiliation

The Gov-CSIRT Indonesia is a part of BSSN, therefore it is fully funded by state budget.

### 3.4. Authority

Based on the Presidential Regulation of the Republic of Indonesia Number 53 Year 2017 concerning BSSN as amended by the Presidential Regulation of the Republic of Indonesia Number 133 Year 2017, the Gov-CSIRT Indonesia is authorized to respond, to mitigate, to investigate and to perform incident impact analysis, and to carry out post cyber security incident recovery in the government sector.

Appropriate response and recovery activities are dispensed upon the request of the constituencies.

## 4. Policies

### 4.1. Types of Incidents and Level of Support

The Gov-CSIRT Indonesia is authorized to address any kind of cyber security incidents, which occur or threaten the constituents (see section 3.2).

The level of support given by the Gov-CSIRT Indonesia will vary depending on the type and severity of the incident.

### 4.2. Co-operations, Interaction and Disclosure of Information

The Gov-CSIRT Indonesia highly regards the importance of operational cooperation and information-sharing between CSIRT, and also with other organisations which may contribute towards cyber security.

All information received will be kept confidential.

### 4.3. Communications and Authentication

Use unencrypted e-mail and telephone for unclassified communication and use PGP-encrypted e-mail for sensitive/restricted/confidential information exchange.

## 5. Services

### 5.1. Incident Response

The Gov-CSIRT Indonesia assists the constituents to respond and recover from a cyber security incident related to the aspects of:

#### 5.1.1. Incident Triage

a. Determining whether the incident and reporter are authentic
b. Assessing the impact and priority of incident

#### 5.1.2. Incident Coordination

a. Coordinating the incident with the constituents
b. Determining possible cause of the incident
c. Providing countermeasures recommendations based on guidelines/ standard operating procedures that Gov-CSIRT Indonesia has for constituents
d. Coordinating incident with CSIRT or other related parties

#### 5.1.3. Incident Resolution

a. Investigating and analyse the impact of incidents
b. Providing technical recommendations for post-incident recovery
c. Providing technical recommendations to correct system vulnerabilities

Gov-CSIRT Indonesia presenting the government sector incidents statistical data as a serve government sector cyber security information centre.

### 5.2. Proactive Activities

The Gov-CSIRT Indonesia is proactively build the maturity of the government agencies to respond and recover from cyber security incidents through:
a. Cyber Security Drill Test
b. Workshop or Technical Guidance
c. Assistance in forming CSIRT Organization

## 6. Reporting Incident

Cyber security incident report can be sent to bantuan70[at]bssn.go.id by attaching:
a. Photo/scan of identity card
b. Incident's evidence, such as photos or screenshot or log file found

## 7. Disclaimers

None Available