R F D

RESULTS-FRAMEWORK DOCUMENT

for

ICERT

Department of Information Technology

(2011-2012)

SECTION 1:

Vision, Mission, Objectives and Functions

Vision

Proactive Contribution in Securing India's cyber space

Mission:

To enhance the security of India's Communications and Information Infrastructure through reactive and proactive action and effective collaboration with cyber users and industry.

Objectives:

- Preventing cyber attacks against the country's cyber space
- Responding to cyber attacks and minimizing damage and recovery time
- Reducing 'national vulnerability to cyber attacks
- Enhancing security awareness among common citizens

Functions:

In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents

- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

SECTION 2:

Inter se Priorities among Key Objectives, Success indicators and Targets

(1st April 2011 – 31st March 2012)

Column 1	Column 2	Column 3	Column 4		Column 5	Column 6				
Objective	Weight	Actions	Success Indicator	Unit	Weight	Target / Criteria Value				
						Excellent	Very Good	Good	Fair	Poor
						100%	90%	80%	70%	60%
Objective 1 Preventing cyber attacks against the country's cyber space	40	**Action 1** Improving the security posture of organisations and cyber users and enhancement in the ability of IT systems to resist cyber attacks	Release of Upgraded 'Crisis Management Plan for countering cyber attacks and cyber terrorism	Date	10	25 Feb 2012	5 March 2012	15 March 2012	25 March 2012	31 March 2012
			Conducting Security audits of critical sector organisations	Number	10	5	4	3	2	1
			Conducting cyber security mock drills at national level and participation in international drills	Number	10	4	3	2	1	-

		Action 2 Conducting awareness trainings for exposure	Number of topics covered for awareness trainings	Number	10	20	18	16	14	12
Objective 2 Responding to cyber attacks and minimizing damage and recovery time	20	**Action 1** Security incident response	Average time taken to register, initiate action and provide initial response to a reported security incident	Hours	20	6	12	18	24	30
Objective 3 Reducing national vulnerability to cyber attacks	20	**Action 1** Issuance of security alerts on latest threats and vulnerabilities	Average time taken to issue security alert upon recognizing the issue	Days	20	2	3	4	5	6
Objective 4 Enhancing security awareness among common citizens	9	**Action 1** Publicize the security site for common citizens	Number of Publicity insertions in media	Number	9	4	3	2	1	1

Mandatory Success Indicators

	Objective	Actions	Success Indicator	Unit	Weight	Excellent 100%	Target/Very Good 90%	Criteria Good 80%	Value Fair 70%	Poor 60%
1	Efficient Functioning of the RFD System	Timely submission of RFD for 2011-12	On-time submission	Date	2	March 31 2011	April 3 2011	April 4 2011	April 5 2011	April 6 2011
		Timely submission of Results for 2011-12	On-Time submission	Date	1	May 1 2012	May 3 2012	May 4 2012	May 5 2012	May 6 2012
		Finalize a Strategic Plan for RC	Finalize the Strategic Plan for next 5 year	Date	2	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
		Identify potential areas of corruption related to organization activities and develop an action plan to mitigate them	Finalize an action plan to mitigate potential areas of corruption.	Date	2	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
		Implementation of Sevottam	Create a Sevottam complaint system to implement, monitor and review Citizen's Charter	Date	2	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
			Create a Sevottam Complaint system to redress and monitor public Grievances	Date	2	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
				TOTAL WEIGHT=	**11**					

SECTION 3:

Trend Values for Success Indicators

Objective	***Actions***	Success Indicator	Unit	Actual Value for FY 09-10	Actual Value for FY 10-11	Target Value for FY 11-12	Projected Value for FY 12-13	Projected Value for FY 13-14
Objective 1 Preventing cyber attacks against the country's cyber space	**Action 1** Improving the security posture of organisations and cyber users and enhancement in the ability of IT systems to resist cyber attacks	Release of Upgraded Crisis Management Plan for countering cyber attacks and cyber terrorism	Date	31 March 2010	15 March 2011	5 March 2012	5 March 2013	5 March 2014
		Conducting Security audits of critical sector organisations	Number	-	-	4	4	4
		Conducting cyber security mock drills at national level and participation in international drills	Number	4	4	3	3	3

	Action 2 Conducting awareness trainings for exposure	Number of topics covered for awareness trainings	Number	21	27	18	18	18
Objective 2 Responding to cyber attacks and minimizing damage and recovery time	**Action 1** Security incident response	Average time taken to register, initiate action and provide initial response to a reported security incident	Hours	-	-	12	12	12
Objective 3 Reducing national vulnerability to cyber attacks	**Action 1** Issuance of security alerts on latest threats and vulnerabilities	Average time taken to issue security alert upon recognizing the issue	Days	-	-	3	3	3
Objective 4 Enhancing security awareness among common citizens	**Action 1** Publicize the security site for common citizens	Number of Publicity insertions in media	Number	-	-	3	3	3

SECTION 4:

Description and Definition of

Success Indicators and Proposed Measurement Methodology

Success indicators	Description and definition	Measurement methodology
Release of Upgraded 'Crisis Management Plan for countering cyber attacks and cyber terrorism'	The Crisis Management Plan for countering cyber attacks and cyber terrorism needs to be updated yearly once	Date of release of upgraded Crisis Management Plan
Conducting Security audits of critical sector organisations	Security auditing will help in assessing the implementation of security best practices and status of compliance, giving an indication of the security posture	Number of security audits conducted
Conducting cyber security mock drills at national level and participation in international drills	The cyber security mock drills are conducted at the national level to assess the readiness of organizations to withstand cyber attacks. The international cyber security drills enable reinforcing the cooperation and coordination between CERT-In and international CERTs.	No. of Mock drills conducted at national level and number of drills participated at international level per year
Number of topics covered for awareness trainings	The training programmes conducted in different relevant areas of cyber security for targeted audience to enhance their awareness for threats to different systems and suitable countermeasures to prevent the attacks and reduce the risk.	No. of topics covered in different training programmes conducted per year.
Average time taken to register, initiate action	With the advent and growth of Information Technology and associated systems and services, the number of incidents also	Average time taken to register, initiate action and provide initial

and provide initial response to a reported security incident	increase. CERT-In has to register, initiate action and provide initial response to all the incidents reported to it within an average time of 6 hours. The exact time of handling an incident depends on nature and severity of incident.	response to a reported security incident
Average time taken to issue security alert upon recognizing the issue	The cyber security alerts are issued by CERT-In on its website & emails and postal mail in certain cases to appraise organizations and users about specific threats and advise them on suitable countermeasures. The issues are recognized based on information available from constituency, collaborative partners, Industry, external CERTs and security agencies apart from information available on Internet. Alerts are prioritized based on severity of the threat and impact.	Average time taken to issue security alert upon recognizing the issue.
Number of Publicity insertions in media	The website called "secureyourpc.in" is hosted by CERT-In to educate common citizens on cyber security issues. Contents specific to parents, children, women, business and individual users are published on this site. The content is updated periodically to enhance awareness of general users on cyber threats and safeguards. This website needs to be publicized in print and electronic media to increase its outreach.	Number of Publicity insertions in print and electronic media.

SECTION 5:

Specific Performance Requirements from other Departments

Departments	Relevant Success Indicator	What do you need?	Why do you need it?	How much you need?	What happens if you do not get it?
Ministry of Finance	Release of Upgraded Crisis Management Plan for countering cyber attacks and cyber terrorism Conducting Security audits of critical sector organisations Conducting cyber security mock drills at national level and participation in international drills Security incidents handled Average time taken to register, initiate action and provide initial response to a reported security incident Average time taken to issue security alert upon recognizing the issue	Sanction of manpower	CERT-In operates on 24X7 basis. Present manpower strength is 26 and requires to be enhanced significantly in line with the responsibility reposed on CERT-In.	Additional 34 persons	It will affect the achievement and realisation of targets

Concerned Ministries/Departments in Central Government and critical sector organisations	Release of Upgraded 'Crisis Management Plan for countering cyber attacks and cyber terrorism'	Comments on Crisis Management Plan	The Crisis Management Plan envisages different roles and responsibilities to be performed by concerned Ministries / Departments. The plan will be upgraded based on their inputs.		Delays the process of upgradation of Crisis Management Plan
	Conducting Security audits of critical sector organisations	Readiness of critical sector organisations	Critical sector organisations are required to implement CMP and security best practices before audit is conducted		Appropriate assessment of security posture will not be possible
	Conducting cyber security mock drills at national level	Readiness of critical sector organisations	Critical sector organisations are required to implement CMP and security best practices before mock drills are conducted		Appropriate assessment of security posture will not be possible

SECTION 6:

Outcome / Impact of activities of ICERT

1	2	3	4	5	6	7	8	9
S. No	**Outcome / Impact of organisation / RCs**	**Jointly responsible for influencing this outcome/impact with the following organisation(s)/ departments/ ministry(ies)**	**Success Indicator(s)**	**2009-2010**	**2010-2011**	**2011-2012**	**2012-2013**	**2013-2014**
1	Improvement of the security of information and communications infrastructure and effective cyber incident resolution	CERT-In, Concerned Ministries/Departments in central government, States/UTs and their critical sector organisations	Release of updated CMP	31 March 2010	15 March 2011	5 March 2012	5 March 2013	5 March 2014
		CERT-In, Concerned Ministries/Departments in central government, States/UTs and their critical sector organisations	Number of security audits of critical sector organisations conducted	-	-	5	5	5
		CERT-In, Concerned Ministries/Departments in central government, States/UTs and their critical sector organisations	Number of cyber security mock drills conducted at national level	4	4	4	4	4
		CERT-In	Average time taken to register, initiate action and provide initial response to a reported security incident			6 Hrs	6 Hrs	6 Hrs
		CERT-In	Average time taken to issue security alert upon recognizing the issue			2 days	2 days	2 days
		CERT-In	Number of skill and awareness enhancement programmes conducted on cyber security	21	27	20	20	20