REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DICT Computer Emergency Response Team (CERT) Manual

Contents

Chapter 1.0 General Information

1.1 Introductions

The age of information and communication technology has made it possible for information and communications to be processed quickly and the speed of accessing the availability of information and data has become convenient for everyone else. The cyber space allowed the creation of virtual communities and the internet became the superhighway for converging information and data. Because of the vastness of the virtual environment, even when it is an internal virtual environment created to perform tasks and processing of information for an organization, it has become exposed to various variables of threats, risks and vulnerabilities.

The increase on computer security incidents and events globally can affect individuals and organization alike, whether accidental or deliberate. These incidents and events may have minimal to catastrophic adverse effect to the individual, group or organization, depending on the impact. Thus, Computer Security has become a major concern for everyone else.

The speed and efficiency in responding to any computer security incident or event is crucial to containing, controlling and minimizing the associated costs for maintaining, recovering or ensuring the continuity of operations at a normal or acceptable environment. With this in mind, the Computer Emergency Response Team (CERT) Manual was developed as part of the preparation in creating the Computer Emergency Response Team Management Plan of the Department of Information and Communications Technology.

During the developmental stage of manual creation, general policies were established and the processes, procedures and protocols involved when responding to computer security incidents and events were planned, documented and reviewed to determine appropriate response plan and management to various incident scenarios.

The planning and development of this manual include referencing with applicable laws and regulatory issuances, ISO/IEC International Standards on Information Technology, international framework from other CERT bodies, documented best practices of establishing, managing and operationalizing CERT from other countries, publicly and internet available published documents on standards and practices related to computer security and other related reference materials.

1.1.1 Purpose

The purpose of this document is to provide the framework for the incident response plan which will become the basis for creating the CERT of each organization. This can also be used as one of the primary reference document by other groups interested to form their own CERT by replicating or duplicating the established processes, procedures and protocols and make the necessary improvement and configuration to conform to the needs and requirement of their organization as far as applicable.

1.1.2 Brief Overview of the Manual

This manual was divided into several Chapters and Sections designed for efficiency in locating any information. The way topics and subjects were clustered together is with the intent to also provide ease in updating and revising any documents within without having to rewrite the entire manual.

1.1.3 Applicability

This manual is applicable to all personnel assigned under the computer emergency response team management including internal and external groups and individuals employed by DICT.

1.1.4 Education and Awareness

An awareness campaign must be conducted with the internal and external stakeholders of DICT. External groups must be provided ample information campaign, brochures and materials including excerpts from the manual that describes its purpose, services offered and how to make use of the CERT Services.

1.2 References

ISO/IEC 27000	Information technology — Security techniques — Information Security Management Systems — Overview and vocabulary
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls
ISO/IEC 24762	Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
ISO/IEC TR 18044	Information technology – Security techniques – Information security incident management
NIST SP 800-61 Rev.2	National Institute of Standards and Technology – Computer Incident Handling Guide
NIST SP 800-30 Rev.1	National Institute of Standards and Technology – Information Security
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems

NOTE:
**Latest version of the above references is to be deemed applicable.*

1.3 Terms and Definitions

Purpose

The purpose of this section is to define related terms used in R.A. 10175, R.A. 10844, and information security management system (ISMS) to ensure that all users have common and basic understanding and interpretation of the words or terms found all throughout this manual.

Scope

The terms and definitions provided in this manual covers commonly used terms and definitions in the ISMS.

Attack
Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organization.

Asset
Any item that has value to the organization

Attribute
Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

Authentication
Provision of assurance that a claimed characteristic of an entity is correct

Authenticity
Property that an entity is what it claims to be

Availability
Property of being accessible and usable upon demand by an authorized entity

Business Continuity
Procedures and/or processes for ensuring continued business operations

CERT
Computer Emergency Response Team (CERT) or Computer Security and Incident Response Team (CSIRT) refers to “an organization that studies computer and network security in order to provide incident response services to victims

of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security". At present, "both terms (CERT and CSIRT) are used in a synonymous manner" (ENISA, 2015 and ENISA, 2015a).

Computer security also known as cyber security or IT security
Is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide

Confidentiality
Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consequence
Outcome of an event affecting objectives.

Control
Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

Control Objective
Statement describing what is to be achieved as a result of implementing controls.

Corrective Action
Action to eliminate the cause of a detected non-conformity or other undesirable situation.
Data
Collection of values assigned to base measures, derived measures and/or indicators. This definition applies only within the context of ISO/IEC 27004:2009.

Electronic Discovery (e-Discovery)
is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing Electronically Stored Information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries.

Effect
Is a deviation from the expected — positive and/or negative.

Effectiveness
Extent to which planned activities are realized and planned results achieved.

Efficiency
Relationship between the results achieved and the resources used.

Event
Occurrence or change of a particular set of circumstances

Guideline
Description that clarifies what should be done and how, to achieve the objectives set out in policies.

ICT systems
Hardware, software, firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.

Information security
Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information security event
It refers to an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information security incident
It is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threating information security

Information system
Application, service, information technology asset, or any other information handling component

Infrastructure
Facilities and equipment to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls

Integrity
Property of protecting the accuracy and completeness of assets

Management
Coordinated activities to direct and control an organization

Management system
Framework of guidelines, policies, procedures, processes and associated resources aimed at ensuring an organization meets its objectives

Measure
Variable to which a value is assigned as the result of measurement

Measurement
Process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria

Object
Item characterized through the measurement of its attributes

Organizations
Entities which utilize ICT DR services

Owner
Identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. This term does not mean that the person actually has any property rights to the asset.

Policy
Overall intention and direction as formally expressed by management

Procedure
Specified way to carry out an activity or a process

Process
Set of interrelated or interacting activities which transforms inputs into outputs

Record
Document stating results achieved or providing evidence of activities performed

Reliability
Property of consistent intended behavior and results

Review
Activity undertaken to determine the suitability, adequacy and effectiveness (2.22) of the subject matter to achieve established objectives

Review object
Specific item being reviewed

Risk
Combination of the probability of an event and its consequence

Risk acceptance
Decision to accept a risk

Risk analysis
Process to comprehend the nature of risk and to determine the level of risk

Risk assessment
Overall process of risk identification, risk analysis and risk evaluation

Risk management
Coordinated activities to direct and control an organization with regard to risk.

Stakeholder
Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Third party
Person or body that is recognized as being independent of the parties involved, as concerns the issue in question

Threat
Potential cause of an unwanted incident, which may result in harm to a system or organization

Validation
Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Verification
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vulnerability
Weakness of an asset or control that can be exploited by one or more threats

1.4 Acronyms and Abbreviation

BIA Business Impact Analysis

CERT Computer Emergency Response Team

CSB Cybersecurity Bureau

DICT Department of Information and Communications Technlogy

DDoS Distributed Denial of Service

FW Firewall

ICT DR Information and Communications Technology Disaster Recovery

IDS Intrusion Detection System

IEC International Electrotechnical Commission

ISMS Information Security Management System

NCERT National Computer Emergency Response Team

SMTP Simple Mail Transfer Protocol

ISO International Standards Organization

MDF Main Distribution frame

PDA Personal Digital Assistant

POC Point of Contact

SIEM Security Information and Event Management

UPS Uninterrupted Power Supply

Chapter 2.0 National Computer Emergency Response Team Structure

Introduction

This section shall provide the organizational structure (See Annex A) to guide the organization in the planning, formulation, development, implementation, management and review of the National Computer Emergency Response Team (NCERT). It will describe the key roles and responsibilities of assigned owners and provide clear scope of accountabilities of individuals, team members and groups (internal and external) that will be involved in the development of the guidelines in the implementation of the national computer emergency response team management plan, treatment and structured approach for responding to information security incident, and the creation of the NCERT.

The factors critical to the successful implementation of the computer emergency response plan are, but not limited to the statement indicated within this document, the following:

1. An established information security policy, objectives and activities that reflect the mandate and functions of CSB including its business objectives to respond with adequacy and readiness when incident or event occurs.

2. An established approach and framework of implementing, maintaining, monitoring and improving computer emergency response plan that is consistent with the organizational requirement and culture.

3. A good understanding of the information security requirements, risk assessment and risk management to respond with appropriate course of action that will direct the NCERT on implementing and managing the computer emergency response plan.

4. Continuous monitoring and evaluation of the performance in the implementation of the NCSP including review of data collected and gathered at regular intervals for improvement.

Section 2 Roles and Responsibilities – Cybersecurity Bureau

Scope
The scope of this section shall cover the roles and responsibilities of members assigned with ownership on tasks specific to the guidelines developed for the management of computer emergency response plan.

2.1 Critical Infostructure Evaluation and Cybersecurity Standards Monitoring Division

This division shall ensure that cybersecurity policies, plans and standards are formulated, implemented, monitored and evaluated. It will also be responsible for monitoring and evaluating the outputs, outcomes and strategic impact of all cybersecurity programs and projects, including the NCERT, towards providing strategic recommendations.

Functions of this division in relation to the NCERT include, but not limited to the following:

a. Review and evaluate the performance of the NCERT;

b. Review and evaluate the results of NCERT operations;
c. Review and evaluate the results from the analysis conducted on the data collected, gathered and added into the database for incidents/event and the corresponding immediate responses made by the NCERT;

d. Evaluate the policies, procedures and processes to determine its applicability and effectiveness in addressing and responding to an incident or event by:

1. Providing guidance in the appropriate changes based from the results from review activities and the actual services offered by the NCERT (Refer to Guidelines for NCERT Services).

2. Providing the framework for implementing changes for the continuous improvement on the NCERT.

3. Recommending appropriate plans to be formulated and implemented to ensure that the elements under NCERT is compliant with applicable local/international standards on Information Technology and obligatory laws and regulations.

4. Evaluating consolidated results from lessons learned in the implementation of the NCSP to:

i. Provide guidance of the best practices in addressing cybersecurity of the organization;

ii. Provide communication plans that is disseminated throughout the organization; and

iii. Benchmark with other international and local organizations, both from private and public institutions to ensure currency and relevancy of the critical elements under the NCSP.

e. Develop well-structured process for detecting, reporting, assessing and managing information security events and enabling tools, methodologies and practices for:

1. Rapid identification and response to any information security event or incident;

2. Improving overall security through quick identification and implement consistent solution; and

3. Providing means of preventing future similar information security incidents.

f. Formulate and develop well-structured approach in the implementation of the NCSP to reduce adverse business impact and help ensure that the mission, organization functions and obligations, business processes, and daily operational activities of CSB are continuously working in place and prevent longer term losses arising from damaged reputation and credibility.

g. Develop well-structured approach to incident response that will create better focus on incident prevention within an organization.

h. Develop well-structured approach to incident response that will provide guidance and direction for prioritizing appropriate course of actions when conducting computer emergency investigations.

i. Develop well defined and structured approach to incident response that will help justify and simplify the allocation of budgets and resources within involved organizational units.
j. Develop structured approach to NCSP to prepare communications plan that will provide better focus on information for information security awareness programs.

k. Provide input to computer emergency response policy review by:

1. Providing data collected from reported security incidents and immediate responses by the NCERT;

2. Updating and strengthening of capability and capacity to collect and gather information on information security incidents and events; and

3. Consolidating data for availability and ease of access of the members of the NCERT.

2.2 National CERT Division

The Division is responsible in receiving, reviewing, and responding to computer security incident reports and activities. This division will also ensure that a systematic information gathering/dissemination, coordination and collaboration among stakeholders, especially computer emergency response teams, are maintained to mitigate information security threats and cybersecurity risks.

Primary functions include the following:

a. Collecting and gathering data during initial report of detected event or incident

b. Creating initial information classification, approving decisions regarding controls and access privileges

c. Perform periodic reclassification

d. Ensure regular reviews for value and updates to manage changes to risk

2.2.1 Roles and Responsibilities

Role	Function	Duties and Responsibiliies
NCERT POC	This level provides 24/7 frontline service for CSB in the implementation of the Computer Emergency Response which establishes the first POC with users or reporters of	1. Receive calls and act as the switchboard operator; 2. Screen and filter data for information classification; 3. Communicate relevant call to NCERT Team Leader; and 4. Provide administrative support to the operation of the team.

	any detected incident or event	
NCERT Analyst	Individuals assigned on this level perform analysis and evaluation of information to determine the relevance which will prompt immediate response and initiate series of actions to respond to the incident or event.	1. Initial collection and data gathering of information on detected and reported incident or event; 2. Creating initial information classification; 3. Opening and assigning incident report ticket number upon classifying information as relevant; 4. Closing of incident report ticket number when information is classified as false positive; 5. Communicating results to personnel or group of personnel with specific task to respond to the incident or event; 6. Perform appropriate responses with the immediate objective of deescalating level of vulnerability and adverse impact to the organization; 7. Logging of responses and actions taken to update the database; and 8. File incident reports on assigned cases.
NCERT Team Leader	Individuals assigned on this level perform supervision and evaluate reported incidents before assigning caseloads to Analyst with appropriate set skills in performing analysis and evaluation of the data gathered and collected during the initial reporting stage.	1. Assign caseloads to NCERT Analyst; 2. Ensure regular review for value and updates to manage changes to risk; 3. Monitor close/open incident report ticket, resolved/unresolved incidents or events; 4. Ensure that appropriate responses are immediately implemented and communicated to personnel tasked to perform specific roles; 5. Ensure that frontline personnel and analysts log and update records immediately and accordingly; 6. Makes the decision to escalate or de-escalate incidents per assessment; 7. Evaluate the performance of Analysts and POCs; and 8. Prepare summary of daily reports.
NCERT Supervisor	Personnel assigned on this level supervise the NCERT team and external groups assigned to perform support services in responding to information security incidents or events.	1. Interface and report to the Director a summary of incident response activities and series of actions taken by NCERT; 2. Evaluate the performance of the NCERT Team Leader to assess efficiency of responses and the effectiveness of the established guidelines, procedures, and processes; 3. Regular review of collected and gathered data to evaluate information value; 4. Submit summary of resolved and unresolved cases to the management for input during review and improvement of the information security incident response plan; 5. Submit analysis results of incidents classified as false positive for input during review to determine the capability of frontline personnel in collecting and gathering substantial information; 6. Evaluate competency of personnel assigned to NCERT to recommend training programs development for competency building of the NCERT Team; and 7. Prepare reportorial requirements for operational, administrative and budgetary purposes.
Systems Compliance and Management Auditor	The Auditor is in charge of information security and IT system compliance including evaluation of the	1. Evaluate whether the internal controls are designed and operating as contemplated in the assessment control risk; 2. Validate and confirm the assessment of control risks based on substantive procedures and other

	implementation in processes and procedures.	audit evidence obtained during the conduct of the audit; 3. Discuss with the Management and agree on the Audit Plan, Audit Methodologies, Resources, Timeframe and reporting requirements for the assignment; and 4. Make Management aware as soon as practical and at an appropriate level of responsibility of material weaknesses in the design or operation of the internal control systems that have come to the Auditor's attention.

2.3 Digital Certificate Division

Administer the Philippine National Public Key Infrastructure (PNPKI) that governs the utilization of Digital Certificates and Signatures of the country.

Primary functions include the following:

a. Provide guidance and policies on the technical aspects of utilizing Digital Signatures and Certificates.
b. Technical support on the efficient use of Public Key Infrastructure.

Chapter 3.0 General Policies

Introduction
Computer and information security is critical to any government, private, or individual, from both public and private organizations. Everyone depends on information technology and information systems to successfully carry out their missions and business functions.

Information systems are subject to threats including incidents and events that can have an adverse effect on organizational operations, assets, individuals, other organization, and the Philippine Government when both the known and unknown vulnerabilities are exploited compromising the confidentiality, integrity or availability of the information being processed, stored, or transmitted by these systems. It is important that these threats are detected and reported at earlier stages and those agency heads at all levels understand their responsibilities.

Scope

1. The scope of this section includes the protection of the confidentiality, integrity and availability of information.

2. The framework for managing information security policy and reporting of information security incidents apply to all organization entities and workers and other involved person and all involved systems throughout the DICT.

3.1 General Policy on NCERT Documentation

a. It is the policy of CSB that information in all its form whether written, spoken or recorded electronically or printed, shall be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle.

b. All policies and procedures shall be documented and made available to individuals responsible for their implementation and compliance.

c. All documentation, which include electronic form, shall be retained for at least six (6) years after its last revision pertaining to policies and procedures, after changes have been made or if any specific policies on records archiving and disposition provide a retention period different from that established by the records disposition schedule of the organization, the retention period established by law or regulation shall govern.

d. All documentation shall be periodically reviewed at regular intervals to ensure its continued appropriateness and applicability over a period of time.

3.2 Policy on NCERT Accountability

a. It is the policy of CSB to ensure the integrity and reliability of the government's digital presence and corporate identity as part of its commitment to good governance. The CSB shall provide a cost efficient service and set of

standards, which shall serve as means for actors both within and outside of government to enforce and accountability.

b. Establish control in reporting all computer emergency incidents and events through appropriate channels with the creation of the NCERT.

3.3 Policy on Establishing the NCERT

a. CSB is mandated to establish NCERT and assign individuals dedicated to work as full time members.

b. Establish the guidelines for handling reported computer emergency incidents and events.

c. Computer emergency incidents and events shall be classified for information systems based on the potential impact on an organization in the event of incidents which endanger the information.

d. Processes and procedures established by CSB for detecting and reporting the occurrence of information security events shall be implemented and observed accordingly.

e. All reported incidents must be identified to initiate immediate response actions to deal with the information security incident.

f. All incident reports shall be updated and collected into the NCERT database.

g. All incidents that have been resolved or closed must be reviewed.

h. Review outputs from NCERT for process improvement.

Chapter 4.0 Protocols and Classifications

Introduction

The CSB has established protocols to activate the NCERT once an incident report is received. This section also contains classification of reports that will be used as reference when assessing incidents and planning appropriate activities and responses.

4.1 Activation of NCERT Protocol

Scope

This section covers the NCERT Protocol of CSB in responding to incident reports.

a. Activate NCERT protocol within 24 hours after confirmation of the validity of the incident.

b. Proper coordination between relevant NCERT personnel should be established to ensure their knowledge of the information security incident is current and up-to-date.

c. Notification chart shall be observed and followed accordingly.

4.2 Assessment Protocol

a. The NCERT Analyst shall determine the category and severity of incident and conduct coordination with the NCERT Team Leader;

b. The NCERT Team Leader shall discuss and determine the next course of action;

c. Upon assembling the NCERT Team, the assessment is executed and reviewed to ensure all pertinent facts are established;

d. All discussions, decisions and activities are to be documented; and

e. Designated persons will take action to notify appropriate internal and external groups, as necessary:

1. Internal Communication

i. On duty team members shall notify all team members;

ii. NCERT Team Leader shall notify all concerned and provide on-going status;

iii. NCERT Team Leader shall issue and direct all sensitive internal communications; and

iv. POC will issue all public internal communication.

2. External Communication

i. All external communication and notification shall be approved by the Cybersecurity Bureau;

ii. The CSB shall establish communication with relevant Third Party, as appropriate for the circumstance;

iii. The CSB shall notify appropriate agencies including LEA's;

iv. NCERT members shall assist in determining if other parties should be notified (e.g. ISPs); and

v. The CSB shall determine if, how and when media should be notified, and respond to all inquiries from the media.

3. Report Originator Notification

i. The Report Originator is informed that the incident has been reported, recorded, and investigation is in progress;

ii. The Report Originator is provided with feedback and updates of the status of the investigation on every completed stage of the incident response information required to escalate or de-escalate the process; and

iii. Report Originator is notified of results, closure of investigation, and recommendation.

4. Status

i. The NCERT shall assume responsibility for preparing and issuing communications within 48 hours after completing stages in an incident response activity to NCERT members, NCERT Management, CSB and other interested parties;

ii. Communications include meetings, video conferencing, teleconferencing, email, telephone, voice recordings, fax, or other means deemed as appropriate; and

iii. Frequency and timeliness of communications are established and revised throughout the life cycle of the incident.

4.3 Containment Protocol

a. The NCERT shall determine the cause and prompt the execution of appropriate activities and processes required to quickly contain and minimize the immediate impact to DICT, the Report Originator, and other relevant stake holders (if applicable)

b. Containment activities designed for execution have the following objectives:

1. Counteract the immediate threat;

2. Prevent propagation or expansion of the incident to other system of the organization;

3. Minimize actual and potential damage;

4. Restrict knowledge of incident to authorized personnel only; and

5. Preserve information relevant to the incident.

4.4 Corrective Measures Protocol

a. The NCERT shall determine and prompt the execution of appropriate activities and processes required to quickly restore state into acceptable operation and secure state,

b. Corrective measure designed for execution has the following objectives:

1. Secure processing environment; and

2. Restore processing environment into its acceptable and secure state.

4.5 Closure Protocol

a. The NCERT shall be actively engaged throughout the life cycle of the information security incident;

b. The NCERT shall continuously assess the progress/status of all containment and corrective measures; and

c. The NCERT shall determine at what point the incident is considered closed or resolved.

4.6 Post Incident Review Protocol

a. All information security incidents related activities are reviewed at regular intervals;

b. All members of the NCERT primary and secondary teams should participate:

1. The NCERT shall host the post incident review after each incident has been resolved and should be scheduled within 2 to 3 weeks after the incident has been remediated; and

2. NCERT review shall consist of the examined incident and all related activities with the objective of improving and polishing the over-all incident response process.

c. Recommendations, discussions and assignments on changes to policy, processes, protocols, procedures or guidelines are documented for distribution to the NCERT members; and

d. NCERT shall conduct the follow up with the report originator, third parties or other relevant stakeholders, as required or as appropriate.

Chapter 5.0 General Guidelines

Introduction

NCERT shall offer and provide various services related to information security.

5.1 List of NCERT Services

Scope

This section shall cover the type of services that the NCERT will provide. It shall also serve as reference material for capacity and capability development that will strengthen the ability of NCERT to respond to any incident or event.

a. Incident Response – Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security.

b. Actionable Security Intelligence - is the real-time collection, normalization, and analysis of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.

c. Signal Intelligence – Intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.

d. Early Warning System – Cyber-attack warning system can be a powerful tool as an early warning system for related attacks, both physical and virtual. A common technique now being used by attackers is to use a denial of service attack as a distraction while another more sinister attack actually takes place.

e. ICT Equipment Testing Lab – A local test laboratory contributes to the development of the national industry by providing inputs that enable projects validation and improvement. In addition, a test laboratory promotes the growth of knowledge and supports the regulatory agencies in the certification process.

f. Web Intelligence (WEBINT) - exploits Artificial Intelligence (AI) and advanced information technology on the Web and Internet. It is the key and the most urgent research field of IT for business intelligence. WEBINT is a means to efficiently identify the intelligence available in open source (OSINT). Structuring and visualizing web-based information allows an analyst to surface tactical information like technical indicators, and strategic understandings like the swaying sentiment of a troubled region.

5.2 Guidelines on Orientation and Preparation of NCERT Personnel

Introduction

This section establishes the guidelines that shall prepare the personnel tasked and assigned to manage and handle responses on information security incident or event. It will provide ample preparation for each person with specific roles to play and provide direction for other members of the team for implementing the NCERT.

Scope

This section shall cover information and guidelines for preparing people, personnel and the team assigned with the task of responding to any incident or event and implement the national computer emergency response team management plan.

Target Audience

This section is intended for personnel who are:

1. Assigned as the POC or tasked to receive, collect and compile reported cases of events during the initial contact (whether human means or automated); and

2. Responsible for managing, supervising and directing the members of the NCERT.

a. Orientation of personnel assigned as the initial POC shall include:

1. Familiarity with the forms that are used for first and second assessment;

2. Familiarity with the different classification and taxonomy used for incident response;

3. Familiarity with the key processes of incident response;

4. Familiarity with the flowchart of handling the incident response;

5. Familiarity with the protocols when communicating and endorsing information collected and compiled for second assessment to members of the NCERT;

6. Importance of proper logging and recording of the event, e.g. accuracy of time stamping, source of event, person reporting, etc.;

7. Importance of updating and recording of events into the database system for information security including recording of data on “false alarms” for future references; and

8. Importance of the time to take to log the report for first assessment will also affect the ability of the NCERT to respond effectively.

b. Orientation for personnel assigned to the NCERT and tasked to respond to incidents or events detected or reported after the initial POC shall include:

1. Familiarity with the forms that are used for first and second assessment;

2. Familiarity with the different classification and taxonomy used for incident response;

3. Familiarity with the key processes of NCERT;

4. Familiarity with the flowchart of handling incident response;

5. Familiarity with the communication protocols after event evaluation and early impact assessment has been conducted and endorsed to the NCERT for escalation for further assessment and/or decisions that are required;

6. Importance of correct and appropriate logging of record and data for later analysis; and

7. Importance of updating the information security event or incident database.

c. Orientation of personnel assigned with the responsibility of managing the NCERT shall include:

1. Implementation of a regular monitoring system to track and monitor all reported incidents and events;

2. Review procedure for evaluating applicability of the NCERT;

3. Treatment and handling procedures for internal security breach protocols;

4. Training program requirement for continuous development and capability building for personnel;

5. Communication plans with other stakeholders;

6. Escalation processes and procedures; and

7. Activation procedures for crisis management.

5.3 Guidelines on Reporting and Submitting Incident Reports

Introduction

As discussed from previous sections, time is an important factor that will determine the ability of the NCERT to respond to any reported event. Providing initial information about an information security event and determining the information security incident will prompt the appropriate people to respond according to the situation and urgency of the response requirement.

Scope.

This section provides the general guidelines on reporting, completing and submitting an information security event and incident.

a. If the person suspects an information security event is in progress or may have occurred with particular emphasis on events which may cause substantial loss or damage to the organization, report should be completed and submitted immediately;

b. The information provided shall be used to initiate appropriate assessment which will determine whether the event is to be categorized as an information security incident or not and if remedial measures are necessary to prevent or limit any loss or damage;

c. If the person reviewing the already completed or partly completed form is assigned to analyze the reports, the event needs to be categorized whether it is an information security incident or a false alarm;

d. If the person reviewing the information security event and incident forms is a member of the NCERT, then the incident form should be updated as the investigation progresses and related updates made to the information security event/incident database;

e. As much as possible, the form should be completed and submitted electronically, including when it is thought possible that the system is under attack and reporting forms can be read by unauthorized people, then alternative means of reporting should be used:

1. Alternative means or forms of reporting include in person, by telephone, by text messaging or by facsimile;

2. Provide information that are only factual and avoid speculating in order to complete the fields within a specified time period (Please refer to Phase 2 Procedure) where it is appropriate to provide information that cannot be confirmed, state clearly the information that is unconfirmed and annotation of information that may lead to what may be true;

3. Always provide full contact details when submitting the completed form. There may be a necessity to contact the person who filed the report either very soon or at a later date to obtain further information concerning the report;

4. Information that were provided during the report discovered to be inaccurate, incomplete or misleading at a later date are amended and resubmitted to update the record and log the correct information into the database; and

5. Closure of report will update the database or if the event has not been fully resolved and tagged as open, the record are still updated.

5.4 Guidelines on Handling Incident Response

Introduction

This section establishes the guidelines for handling responses on information security incident or event. It provides direction in determining whether the information security events become information security incidents. When an occurrence of an information security event is detected and reported by (human or automatic means), the event will initiate series of phases and stages prompting the NCERT to respond accordingly.

Scope

This section covers only guidelines on handling reported incidents and events for Information Security.

Target Audience

This section is intended for personnel who are:

1. Assigned as the POC or tasked to receive, collect and compile reported cases of events during the initial contact (whether human means or automated).

2. Responsible for managing, supervising and directing the members of the NCERT.

a. Detection Reporting

1. Incident events detected and reported either by human or automated feed shall be immediately logged into the information security incident monitoring and tracking system;

2. Reported incident or detected event shall be communicated immediately to the NCERT;

3. Communicated reports shall be logged immediately to update records; and

4. Always update the system with changes or responses made associated with the incident report ticket number.

b. Assessment Decision

1. Information gathered and collected are submitted to the NCERT;

2. False positive results from initial assessment shall also be logged into the system to track all reported events and incidents;

3. Team Leaders assigning caseloads to NCERT Analyst shall log and record incident report ticket number to update database;

4. Initial assessment that contains relevant information shall be assigned to NCERT Analyst for further analysis and evaluation;

5. Results from second assessment shall be recorded and logged into the system;

6. Communicate results for immediate response to NCERT members, technical support team, and other external support groups; and

7. Terminate or close incident report ticket number by updating the system when cases are concluded as resolved.

c. Response

1. List of personnel tasked and assigned with specific role in NCERT shall be regularly updated and posted to message boards;

2. Immediate objectives for responding to incidents or events is to lower the level of vulnerability and impact;

i. Adverse impact, risk levels and associated threats and vulnerabilities shall be immediately evaluated and assessed to initiate various controls and appropriate level of responses;

ii. Immediate response shall be documented accordingly;

iii. Reports shall be completed and filed immediately to update the system;

iv. First responders to the reported incident or event on breach of information security shall conduct appropriate turnover procedure;

v. Log appropriate tagging of incident report, e.g. closed/open, resolved/unresolved; and

vi. Immediate responses to reported events and detected incidents shall be evaluated regularly to determine the effectiveness of these responses and improve the system of responding to any information security breach.

5.5 Guidelines on Collecting and Gathering Data

Introduction

This section establishes the guidelines for collecting and gathering data and information for analysis that will direct the NCERT to respond accordingly.

Scope

This section will cover only guidelines on collecting and gathering data for initial and second assessment on reported and detected incidents and events.

Target Audience

This section is intended for personnel who are:

1. Assigned as the POC or tasked to receive, collect and compile reported cases of events during the initial contact (whether human means or automated)..
2. Responsible for managing, supervising and directing the members of the NCERT

a. Guidelines on Collecting and Gathering Data and Information for Analysis

1. Events or incidents that are detected and reported either by human or automated means shall be logged immediately and recorded appropriately into the system;

2. Information, after it has been collected, shall be classified according to information categories;

3. Reported incidents or events shall be classified according to its potential impact to the organization: limited adverse effect, serious adverse effect, or severe/catastrophic adverse effect;

4. These information shall be classified and rated based from its security objectives: Confidentiality, Integrity and Availability of Information;

5. Data or information shall also be evaluated according to the sources of threats which can occur on three levels: the organizational level, the mission or business process level, and the information level;

6. Information that has been collected shall be classified according to its type. This can be adversarial, accidental, structural or environmental in nature;

7. Once data or information is collected, it shall also tagged according to its characteristics and the range of its effect;

i. Information collection and data gathering shall be complete and substantial to provide analyst ample data to perform analysis which will initiate immediate response or prompt series of incident response activities;

ii. Time stamping and recording of event is crucial. It is therefore very important for the person collecting data to determine the time the event or incident occurred or initially detected and reported.

iii. Information that is classified as “false” positive shall be logged and recorded into the database as input for future analysis.

5.6 Guidelines on Acquiring New Information

Introduction

The modern world thrives on information and it is the driving force that now fuels the society. It is crucial to many aspects of business and life of individuals and organizations and therefore should be managed well. This has also led to the evolution of using technology to store, process or transmit information through electronic means.

Scope

This section will provide general guidelines when acquiring information to conduct forensic analysis done by the NCERT of CSB.

Target Audience

This section is intended for personnel who are:

1. Assigned as Analyst tasked to gather, collect, search, review, and analyze information security incident that has been reported;

2. Members of the NCERT; and

3. Responsible for managing, supervising and directing the members of the NCERT.

a. Guidelines for handling e-discovery

1. Adopt a process for reporting information relating to a probable threat of litigation to a responsible decision maker to assist in demonstrating reasonableness and good faith;

2. To determine scope of information that should be preserved, it should be factored into the process of decision making, the amount of information that should be preserved, the nature of the issues raised in the matter of information preservation, the accessibility of information, the probative value of information

and the relative burdens and costs of preservation efforts;

3. Compliance with a legal hold should be regularly monitored; and

4. Any legal hold policy, procedure or practice should include provisions for releasing the hold upon the termination of the matter at issue so that the organization can adhere to polices for managing information through its useful lifecycle in the absence of legal a hold.

Chapter 6.0 General Procedures

Introduction

During the initial stage of the event, process of decision making is already in progress. The information gathered and collected will provide a basis to evaluate and assess the relevancy of information to initiate series of responses to limit.

Scope

This section covers the procedures for the three stages of computer emergency response plan of NCERT.

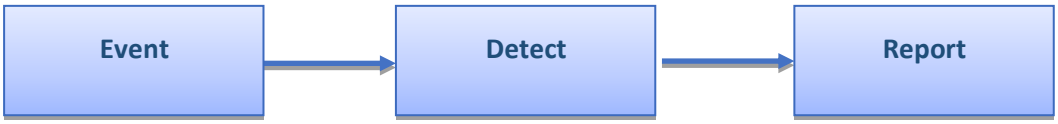
6.1 Detection and Reporting Procedure

Control Objectives

1. Gathering and collecting of information should be identified and evaluated for relevancy of information and made available to the users who need them.

2. Documentation and appropriate logging of records and data shall be maintained for regular monitoring and update of the database.

Stages and Processes



a. Receiving Calls or Reports

1. All calls receive is filtered and directed to appropriate personnel with specific NCERT tasks and responsibilities.

2. All reported calls received are immediately logged into the system after it has been filtered as relevant security information event that will prompt incident response team to initiate series of processes and responses.

b. Detection of Event through Human Means

1. Use Initial Assessment Form (IAF1) to gather and collect data for analysis of relevancy of the information;

   i. Given the potentially time-critical nature of the process, it is not essential to complete all fields in the reporting form at this time.

2. Fill the IAF1 with appropriate information and ensure approximate time is recorded when the event was initially detected;

3. Make sure that the name of the person reporting (if, applicable), the name of the person gathering and collecting information and the person assigned to respond is clearly indicated in the IAF1:

   i. Initial assessment results with relevant information after initial evaluation of the NCERT Analyst are assigned with Case Number and prompted for Second Assessment;

   ii. Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with the roles to respond to a security incident or event;

   iii. Case Numbers with open or unresolved are reviewed and monitored closely to contain and control any other potential adverse impact;

   iv. Case Numbers with close or resolved are logged into the system to update the record; and

   v. Summary of resolved and unresolved cases are reported on a daily and weekly basis.

c. Detection of Event through Automatic Means

1. Use IAF1 to gather and collect data for analysis of relevancy of the information;

2. Fill the IAF1 with appropriate information and ensure approximate time is recorded when the event was initially detected;

3. System or network server clock is used as the official time when event was initially detected;

4. Use IAF1 to gather and collect information for evaluation by the NCERT Analyst;

5. Initial assessment results with relevant information after initial evaluation of the NCERT Analyst are assigned with Case Number and prompted for the Final Assessment Form (FAF1);

6. Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with the roles to respond to a security incident or event;

7. Case Numbers with open or unresolved are reviewed and monitored closely to contain and control any other potential adverse impact;

8. Case Numbers with close or resolved are logged into the system to update the record; and

9. Summary of resolved and unresolved cases are reported on a daily and weekly basis.

6.2 Assessment Decision Procedure

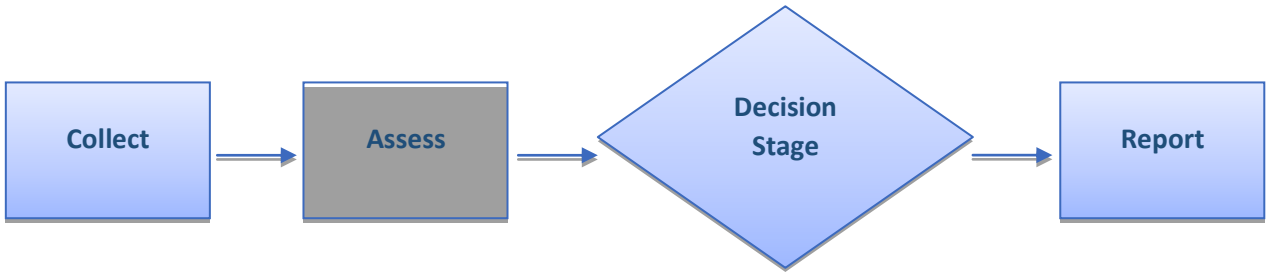
Control Objectives

1. Determine the type of detected and reported incident from false alarm and relevant

2. Classify assessment results according to the degree of loss and the adverse impact it may cause towards the organization

3. Submit interim reports for reported incidents that require longer period of responses

Stages and Processes



a. Initial Assessment and Decision

1. All completed information security event reporting forms are acknowledged by the receiving person;

2. All collected data and information are entered into the information security event/incident database;

3. All reports are reviewed after it has been logged into the system. Seek any clarification from the person reporting the information security event and collect any further information required and known to be available, whether from the reporting person or somewhere else;

4. Assessment is conducted to determine whether the information security event is determined to be a false alarm, a security incident or is in fact a false alarm:

    i. If the information security event is determined to be a false alarm, the information security event reporting should be completed and communicated to NCERT for addition to the information security event/incident database and review, and copied to the reporting person and the manager under which the person is assigned to, with reference to the time zone difference using Philippine Standard Time as reference point:

        a) If reported information security incident or event is identified as local source, response from the reporter should be within 24 hours after it was initially reported.

        b) if reported information security incident or event is identified as international, response from the reporter should be within 48 hours after it was initially reported.

    ii. If the information security event is determined to be likely to be an information security incident, and if the person assessing it has the appropriate level of competence, further assessment must be conducted, otherwise, it should be forwarded to the person with appropriate set skills level to respond to the reported information security incident.

5. When considering the potential or actual adverse effect of an information security incident on the business of an organization, the first step will be to consider which of a number of consequences is relevant:

    i. For information considered to be relevant, the related categories found under Classification of Security Incidents, should be used to establish the potential or actual impacts for entry into the information security incident report.

    ii. All reported information security incidents that are tagged as resolved include details of the safeguards that have been taken and any lessons learned (e.g. safeguards to be adopted to prevent reoccurrence or similar occurrences).

6. Reporting forms that have been completed are referred to the NCERT for entry into the information security event/incident database and review;

7. Interim reports are submitted for investigations likely to be longer than one week;

8. Analyst assigned to assess the information security incident report must know when it is necessary to escalate matters and to whom; and

9. Documented change control procedures are applied in all activities conducted and must be followed.

b. Final Assessment and Incident Confirmation

1. NCERT is responsible for the confirmation or decision to categorize the information security event after the final assessment:

i. The information security incident reporting form must be acknowledged as soon has it has been received;

ii. Enter the form into the information security even/incident database;

iii. Seek clarification from the POC or operations support group to gain more information regarding the incident reporting form;

iv. Review the reporting form content; and

v. Collect any further information required and known to be available, whether from the POC, the person who completed the information security event reporting form, the operations support group or elsewhere:

a) If there is still a degree of uncertainty to the authenticity of the information security incident or the completeness of the information, the NCERT should conduct an assessment to determine of the reported incident is real or is a false alarm;

b) If the reported information security event is determined to be a false alarm:

1) The information security report is completed and logged to update the database system for information security event/incident and communicated to the NCERT Team Leader.

2) Copies of the report should be sent to the POC, the NCERT Team Leader, the reporting person and the local manager of the reporting person.

c) If the reported information security incident is determined to be real then further assessment should be conducted, involving other colleagues with appropriate set skills and confirm the following:

1) How the information security incident was caused, its adverse effects, what has been affected, the impact or potential impact, indication of its significance;

2) Attacks done deliberately by human technical methods and techniques, determine the depth of the infiltration is into the DICT system, service and or network and the level of control the attacker was able to obtain, the data that has been accessed, and the software that has been copied, altered or destroyed by the attacker;

3) Attacks done deliberately through human physical attack on any of the DICT information system, service and/or network hardware and/or physical location, the physical damage whether indirect or direct must be examined and confirmed including the physical access into the facilities;

4) Information security incidents not directly caused by human actions, whether direct or indirect (e.g. physical access open because of fire), should be determined and confirmed;

5) Review state and progress of the information incident security incident has been dealt so far; and

6) Review being conducted on the potential or actual adverse effects of the information security incident on the operations of DICT should be confirmed to determine which of a number of consequences is relevant, (Refer to Classification of Security Incidents).

6.3 Response Procedure

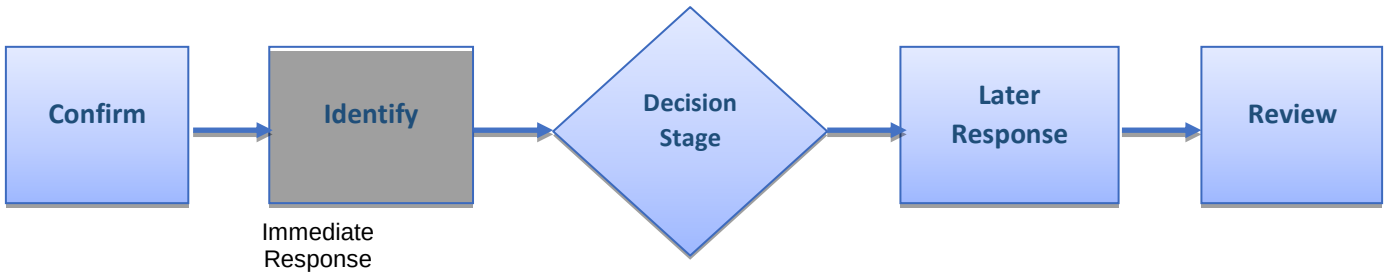
Control Objectives

1. Confirmation of the assessment results on the relevant information to contain, minimize or control the effects of the report on information security incident

2. Identification and execution of immediate or later responses based on the situation

3. Review of the responses (immediate or later responses) including the procedures, processes and the management system for responding to information security incident

Stages and Processes



a. Response

1. Immediate response actions should be identified;

2. Record details on the information security incident form and within the information security event/incident database;

Confirm

. Notify required actions to appropriate persons or groups;

4. Initiation of emergency and permanent safeguards to control or minimize the damage and impact of the reported information security incident;

5. Determine the significance and severity of the information security incident report to NCERT;

6. Notify directly the appropriate senior management when information security incident is deemed to be sufficiently significant or has been elevated to a crisis stage; and

7. Activation of a business continuity plan if “crisis situation” is evident and has been declared.

b. Actions

1. The critical applications and operations of DICT must be allowed to function correctly;

2. Collect as much information as possible about the attacker;

3. Appropriate authentication means are implemented to prevent unauthorized individuals into accessing and attacking the system when emergency safeguards are called into actions;

4. Prioritize prevention of re-occurrence, rectify the safeguard mechanisms through the exposed weaknesses of the attacker, and weigh the gains to justify the effort of tracking the attacker especially when it is non-malicious and has caused little or no damage at all;

5. Information security incident report caused other than by deliberate attack must be investigated to determine the cause;

6. Activation of surveillance techniques to counter the attacks of the hacker or attacker; and

7. Check information that may be corrupted by the information security incident report against backup records for any modification, insertions or deletions of information,
    i. Check integrity of the logs

c. Incident Information Update

1. Always update the information security incident report as much as is possible;

2. Record and add update into the information security event/incident database and notify the NCERT Team Leader and others as necessary. Update includes:

    i. What the information security incident is;

    ii. How it was caused and by what and whom;

    iii. What it affects or could affect in the information system, operations and critical missions of CSB;

    iv. The impact or potential impact of the information security incident on the business and operations of CSB;

    v. Changes to the indication as to whether the information security incident is deemed significant or not; and

    vi. Current state or progress of how the reported information security incident has been dealt so far.

3. If the reported information security incident has been resolved, the report include details of the safeguards that have been taken and any other lesson learned;

4. NCERT is responsible for ensuring the secure retention of all information pertaining to an information security incident for further analysis and potential legal evidential use,

    i. All volatile data are collected before the affected IT system, service or network is shut down for a complete forensic investigation which includes the following actions:

        1) Information to be collected includes contents of memories, cache and registers and details of any processes running;

        2) Full forensic duplication of the affected system, service and/or network, or a low level backup of logs and important files;

        3) Collect and review logs from neighboring systems, services and networks such as routers and firewalls;

        4) Store all information collected on read only media;

        5) Atleast two persons, while the forensic duplication is performed, must be present to assert and certify that all activities that have been carried out complies with the relevant legislation and regulation;

        6) Document the specifications and descriptions of the tools and commands used to perform the forensic duplication and must be stored together with the original media; and

        7) The NCERT member should facilitate the return of the affected facility to a secure operational state that is not susceptible to a compromise by the same attack.

d. Other Activities for Reports Assessed as Significant

1. Institute forensic analysis procedure;

2. Inform and coordinate with personnel responsible for internal and external communications of the facts and the proposals for what must be communicated in what form and to whom;

3. Any information security incident report that has been completed must be entered into the database system for information security event/incident to update records;

4. Interim reports must be instituted for investigations likely to have longer time to undertake;

5. NCERT members must observe and be made aware of the documentation requirements for the following:

   i. The manner of necessity to escalate matters and to whom

   ii. Change management

6. The information security incident report shall be reported in the first instance to relevant people in person, by telephone or text messaging as a contingency plan for communication:

   i. Establish a secure method of communication

   ii. Nominate backup advisors, deputies or representatives in the case of absence

e. Incident Control

1. A review shall be conducted after immediate responses have been instigated to control the incident:

   i. Consult with colleagues if necessary;

   ii. If the reported information security incident is confirmed to be under control, institute later responses, forensic analysis, and communications to close the reported incident and restore normal operations; and

   iii. If reported information security incident is confirmed to be not under control, institute "crisis activities" to activate the crisis management plan.

f. Later Responses

1. Identify the "if and what" further responses are required to deal with the information security incident, including:

   i. Restoring the affected information systems, services and or networks back to normal operations;

   ii. Recording details on the information security incident reporting form;

   iii. Updating the details and information report into the information security incident/event database;

   iv. Notifying the personnel responsible for completing related actions;

   v. Contacting supplier immediately if CSB relies on external vendors for hardware and software and other third party support services;

   vi. Conducting additional monitoring activities after restoring to normal operations to detect other weaknesses or vulnerabilities; and

   vii. Conducting recovery activities when incidents were caused by non-IT related cause.

g. Crisis Activities

1. Institute crisis activities leading to the activation of crisis management plan;

2. Activate fire suppression facilities and evacuation procedures for fire related incidents;

3. Activate flood prevention facilities and evacuation procedures for flood related incidents;

4. Activate bomb "handling" and related evacuation procedures for bomb threat and domestic terrorism related activities; and

5. Activate procedures to put on board specialists such as information system fraud investigators and technical attack investigators for cyber-attacks and intrusion related incidents.

h. Forensic Analysis

1. Avoid having the target being rendered as unavailable, altered, or otherwise compromised by protecting the system, service and/or network during forensic analysis procedure:

   i. Protect against new virus that may be introduced during the conduct of forensic analysis.

   ii. Minimize or no effects will be made on normal operations.

2. Prioritize capture of evidence by proceeding from the most volatile to the least volatile;

3. Identify all relevant files on the subject systems, service, and/or network, including normal files, deleted files, password or password protected files, and encrypted files:

4. Recover discovered deleted files and other data:

   i. Uncover IP addresses, host names, network routes and website information;

   ii. Extract contents of hidden, temporary, and swap files used by both application and the operating system software;

   iii. Access the contents of protected or encrypted files unless it is a possible violation of a law;

   iv. Analyze all possible, relevant data found in special and typically inaccessible data and disc storage areas;

   v. Analyze file access, modification and creation times;

   vi. Analyze system, service, network, and application logs;

   vii. Determine the activity of users and/or applications on a system, service or network;

   viii. Analyze emails for source information and content;

   ix. Perform file integrity checks to detect Trojan horse files and files not originally from the system;

   x. If applicable, analyze physical evidence for possible fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, biometric systems, and interview witnesses; and

   xi. Handle and store the extracted potential evidence by securing and protecting it from being damaged or rendered unusable.

5. Make sure that sensitive information and material cannot be seen by those not authorized to view recovered potential evidence;

6. Evidence gathering must be with the accordance of the rules of the court or hearing, in which the evidence may be presented;

7. Make conclusions on the reasons for the information security incident and the actions required including the timeframe. Provide list of the evidences of relevant files to be included as attachment to main reports; and

8. When required, provide expert support to any disciplinary or legal action that CSB will undertake.

i. Communications

1. Prepare certain information in advance that can be quickly adjusted to the circumstances of a particular information security incident issued to the Media such as:

   i. When security incident is confirmed as real;

   ii. When security incident is confirmed as under control;

   iii. When it is designated for “crisis” activities;

iv. When it is resolved or closed; and

v. When post incident review has been completed and conclusions reached.

2. Prepare the personnel who will be tasked and assigned to communicate with internal (outside of normal NCERT/management communication lines) and media;

3. Information that is to be released must be in accordance to CSB's policy on information dissemination; and

4. Information to be released must be reviewed by the relevant parties of CSB.

j. Improve

1. Review the results of the forensic analysis that were further conducted after the information security incident report has been resolved and closure has been agreed;

2. Conduct further forensic analysis to identify evidence even after the information security incident report form has been completed and viewed as closed or resolved. Same toolsets and procedures must be used for further forensic analysis of evidences;

3. Identify the lessons to be learned once the information security incident has been concluded as closed or resolved, from the initial handling to quick identification up to the level when immediate or later responses were taken. Lessons may include:

i. New or changed requirements for information security safeguards, either technical or non-technical safeguards which may include:

1) Rapid material updates;

2) Delivery of materials or support/shared services;
3) Security awareness briefings for end-users and personnel; and

4) Rapid revision and issue of security guidelines and/or standards.

ii. Changes to the NCERT and its processes, procedures, reporting forms, and information security event/incident database;

iii. Look for patterns or trends beyond a single information security incident to help identify the need for safeguards or approach changes; and

iv. Conduct information security testing and vulnerability assessment.

6.4 Responding to Information Security Report Procedure

Introduction

As part of establishing the national security for information technology, all DICT employees, contractors and third party users will be made aware of the established procedures for reporting different types of even and weakness that might have an impact on the security of organizational assets. Early reporting upon detection will ensure that information security events and weaknesses associated with information systems of CSB are communicated in a manner that allows timely corrective actions to be taken by NCERT. The NCERT is tasked to respond to any reported information security event in a quick, effective and orderly response to mitigate, prevent, minimize, control or correct any vulnerability or threats that may create adverse impact to the organization.

Scope

This section covers the response procedure of the NCERT.

Control Objectives

1. Logging and recording of all activities undertaken when responding to the information security incident.

2. Established procedures must be reviewed to determine applicability and for continuous improvement of the processes, procedures and policies of CSB for information security incident response.

a. Responding to Information Security Incident Report

1. Use Form IAF1 and FAF1 as reference when responding to reported incident or event associated with the information system of CSB.

2. Refer to the guidelines for handling incident response.

b. Procedures for Responding to Different Types of Information Security Incident

1. When responding to information system failures and loss of service:

i. Immediately halt attacks if caught while in progress;

ii. Follow back up procedures;

iii. Assess the extent of operational downtime and determine the earliest time possible to bring the system into a stable operating state;

iv. Check if data or information has been compromised or security breach has occurred during system failure or loss of service;

v. Check records of updates and regular maintenance being conducted such as version of the anti-virus software, installation or updates of patches to correct software vulnerabilities, firewall technology in place, etc.;

vi. Review and monitor systems and determine effectiveness of information security safeguards to detect and correct the breakdowns in security. Monitoring and review may include:

1) Sampling

2) System checks

3) Reports of access to systems

4) Review of Logs

5) Audit Reports

vii. Preserve and gather evidence that results from the incident that has occurred;

viii. In an urgent situation that requires immediate action please refer to the established escalation procedure,

1) NCERT member responding is authorized to secure the asset without the owner's consent when it is determined to be critical in nature:

a) Appropriate logging and recording of artifacts must be conducted.

b) Another member of the NCERT must be present or representative from the reporting party must be around to observe the secure removal of the item from the site.

2. When responding to malicious code attacks

i. Determine fully if a malicious code attack has occurred and this can be evaluated based from some of the examples below:

1) Complaints on slow access to internet, exhaustion of system resources, slow disk access or slow system boots;

2) Numerous alert reports have been generated by Host-based Intrusion Detection System (HID) or by anti-virus or malicious code detection software;

3) Significance in increased network usage;

4) Access violation entries are noticed and observed in perimeter router logs or firewall logs;

5) A detected surge on out-bounced SMTP traffic originating from an internal IP address;

6) Noticeable unusual deviation from typical network traffic flows observed by a system administrator;

7) Security controls such as anti-virus software and personnel firewalls are disabled on many hosts; and

8) General system instability and crashes.

ii. Upon confirmation that there is a malicious code security breach, it is important to collect information about the malicious code;

iii. Identify characteristics of the malicious code to apply appropriate course of actions. Examples are given below:

1) Type of malicious code: network mass, mass-mailing worm, virus, Trojan horse, etc.

2) Vulnerability that is being exploited by the malicious code, services or ports being attacked, etc.

ii. Assess the scope, damage and impact of the outbreak to effectively deal with the incident;

iii. Record all actions taken when dealing with the outbreak and any corresponding results, (Please see General Procedures for Phase 2). Logging should be carried out throughout the whole security incident response process;

iv. Notify all appropriate parties and escalate the incident to the appropriate level following a predefined escalation procedure (Please see Escalation Procedure). The information provided during the escalation process should be clear, concise, accurate and factual. Inaccurate, misleading or incomplete information may hinder the response process or may even worsen the situation; and

v. Carry out containment activities to prevent the malicious code from inflicting further damage through the following:

1) Identify infected systems;

2) Contain the outbreak;

3) Keep record of all actions taken;

4) Execute full eradication process as soon as possible or in parallel with the containment process to prevent files from being corrupted, destroyed or deleted on the infected system.

5) Notify all related parties before the resumption of suspended services. IT personnel must restore specific functions and servers stage by stage in a controlled manner and in the order of demand. Start with the most essential services or those servicing the majority

6) Verify information that the restoration operation has been successful and that all services are back to normal after resuming the suspended services. Additional monitoring may be implemented to watch and observe for any suspicious activity in the network segments concerned.

3. When responding to Distributed Denial of Service (DDoS)

i. Immediately assess and determine the scope and impact to plan for the next course of action to be taken to address the incident.

ii. Determine the intent, capability and target of the attacker to deploy appropriate counter measures and install safeguard mechanisms,

iii. Additional components must be immediately available as replacement in the event of component failure,

iv. Use load balancing mechanism to distribute the force of DDoS attacks between several components and geographic locations to prevent single component or network from receiving the full volume of traffic,

v. Immediately execute the escalation procedure,

vi. Ensure appropriate physical security measures are in place to detect unauthorized entry or access into the site,

vii. Immediately detect or remove reflectors or amplifiers from the network to minimize avenues of anonymity and large scale assault into the system as well as lower the risk for critical infrastructure of the organization,

4. When responding to breaches of confidentiality and integrity

i. Immediately assess the impact and the degree of security breach,

ii. Implement escalation procedure immediately,

iii. Review all logs and records on entry and exit of all personnel with access to critical information system and data processing facilities including data storage facilities,

iv. Change all passwords and entry codes immediately,

v. Record all activities taken for further analysis and improvement of the security systems being implemented,

5. When responding to misuse of information system

i. Trace logs and records of all transactions,

ii. Execute control measures immediately to further prevent any unauthorized access,

iii. Investigate and evaluate the intent and extent of the impact in the misuse of the information system,

iv. Change all passwords and entry codes immediately,

v. Review implementation of security password maintenance, security logs, and security access into the system,

vi. Immediately disconnect the equipment or remove from network connection when unauthorized use or access of the information system has been detected and confirmed,

vii. Record all activities taken for further analysis and improvement of the security systems being implemented.

6.5 Reporting Procedure

Introduction

When an information security event is detected whether by human and automated means and reported immediately, it increases the ability of the NCERT to verify the information and initiate immediate response when it has been determined to be relevant. It is important that the person tasked to receive all reported information security incidents is able to report and notify appropriate personnel. The process of reporting a security information incident is not only limited to reporting the initial report of the event but it is also important to know how to report an incident when it is deemed necessary to escalate the matter to the next level of decision makers.

Scope

This section covers the reporting procedure upon the initial receipt of a report of an information security event or incident, interim reporting and escalated reporting.

Control Objectives

1. Acknowledgment receipt of the information security incident report

2. Recording of the official time stamp of the information security event upon initial report
3. Forms for the following: IAF1 and FAF1

a. Initial Reporting of Information Security Incident Report

1. All calls are filtered by the POC to determine if the call is related to a report on an information security incident;

2. Initial incoming report on information security incident is logged into the system to record and log report into the database for information incident/event database,

3. Initial information from the incoming calls or report is recorded into the IAF1;

4. The IAF1 with partial information is forwarded to the NCERT Analyst for data gathering and collection;

5. The Initial Report is forwarded to the concerned personnel for immediate response and the NCERT Team Leader is informed; and

6. All reports must be updated when it has been closed or resolved to update the system.

6.6 Escalation Procedure

Introduction

Escalation happens when there are circumstances where matters have to be escalated to the senior management, another group or persons within the organization or groups outside the organization. However, it is also important that before the incident is escalated, it must exhaust all means to respond immediately to the incident or it qualifies as an urgent matter that can affect the national security.

Scope

This section will cover procedures on escalation including when, what and who to notify a matter that is being escalated.

Control Objectives

1. Assessment reports to determine the relevance of the reported information security incident;
2. Impact and risk assessment reports that will initiate the decision to escalate matters;
3. Rating scale for vulnerability, threat and predisposing conditions to support and justify the action to escalate; and
4. Escalation request form that will provide paper trail for auditing.

a. Factor to Consider for Escalation

1. When results of the evaluation is determined to have an impact to the national security:

i. When the results of the evaluation have severe or catastrophic adverse impact to the organization;

ii. When the results of the evaluation will is classified as critical and will severely affect the information system level of the organization;

iii. When major issues become evident at the early stages of reporting; and

iv. When information security incident report is a recurring incident after it has been previously resolved.

b. Escalation Procedure

1. Use the rating scale on vulnerabilities and threats to evaluate the degree or gravity of adverse impact to the organization;

2. The decision to escalate will be taken by the NCERT Leader after determining the results of the evaluation;

3. Escalation request must include the following:

    i. The type of event and when it happened;

    ii. The degree of severity or adverse impact to the national level, organizational level or the information system level;

    iii. The name of the person requesting for escalation and the official time stamp and date when escalation requests was made; and

    iv. The case number assigned to the information security incident report.

4. The Analyst shall consult with the Team Leader when major issues are evident during the early stage of assessment;

5. Send an alert message notifying the appropriate personnel to respond to the escalated information security incident report;

6. The Analyst shall consult with the Team Leader when the reported information security incident is required for escalation;

7. The Analyst shall consult with the Team Leader to determine the next course of action whether it should be escalated or forwarded to another group to initiate immediate response or take series of actions;

8. Notification of escalation after assessment results are concluded and Escalation Request is forwarded and submitted to the Team Leader;

9. Escalating the information security incident report must have supporting documents that will justify and rationalize the escalation requests;

10. All escalated information security incident report must be monitored at regular intervals to ensure that it has been properly coordinated and forwarded to the personnel concerned;

11. Escalated information security incident report must be logged into the system to update the information security event/incident database; and

1. A summary of escalated report on information security incident must be prepared and submitted to the NCERT Management for review and evaluation.

c. De-escalation Procedure

1. When the escalated information security incident report is addressed and its classification has been downgraded to manageable and controllable incident, a de-escalation notification is forwarded to:

    i. The original source where the report has emanated

    ii. The reporting Analyst

    iii. The NCERT Team Leader

    iv. The NCERT Supervisor

    v. The NCERT

2. When the escalation request was reviewed and evaluated to determine the impact and severity and was concluded to be manageable, controllable and within the scope of and existing set skills of the NCERT Team, the escalation notification request will be downgraded and forwarded to the concerned personnel with the specific set skills to respond immediately or for later responses.

3. De-escalated information security incident report must be logged into the system to update the information security event/incident database.

6.7 Communication Procedure

Introduction

When information security incident occurs, there are instances that the need to communicate and coordinate with other groups or third parties is very important. So whenever appropriate, such as contacting law enforcement agencies, responding to media inquiries or discussing and sharing information with ISPs and vendors of vulnerable software or other incident response team, the need to establish policies and procedures to ensure that sensitive information will not be disclosed to unauthorized party is required. This is to prevent potentially leading to additional disruption, reputation damage or financial loss. Any communication conducted with outside parties must be well documented for evidentiary and liability purposes.

Scope

This section covers communication procedures with outside parties or external groups during incident response.

Control Objectives

1. Communication policies are developed to ensure that sensitive or critical information are not disclose when communicating and coordinating with parties and groups outside NCERT.

2. Record of communication activities are documented and must be stored and filed in a secure place.

a. Media Communications Procedure

1. All members of NCERT must be oriented and trained on how to interact with media regarding incidents. Included are as follows:

   i. Emphasis on the importance of not revealing important information such as technical details of countermeasures that could assist other attackers;

   ii. Discuss positive aspects of communicating and disclosing important information to the public fully and effectively;

   iii. Hold mock interviews and press conferences to simulate media interaction during incident handling;

   iv. A single POC person must be appointed tasked to respond to handle the media and inquiries;

   v. Disclosure of information must have written approval from the Management to ensure protection of information security;

   vi. All communication with outside parties must be documented accordingly; and

   vii. Media communications procedure must be reviewed at regular interval to determine its applicability, effectiveness and establish continuous improvement.

b. Contacting and Communicating with Law Enforcement Procedure

1. Whenever the situation requires contacting law enforcement agencies, this must be established immediately.

2. Communicating and sharing of information with law enforcement agency must be with written approval from the CSB.

3. Establish a single POC with the LEA or secure alternate contact persons to ensure availability when the need to communicate and coordinate with the agency arises.

4. All communication and coordination activities are recorded and documented accordingly.

c. Contacting Other Groups

1. Communicating and contacting other groups while responding to information security incident must be with written approval from the CSB.

2. A single POC is assigned to have all communication directed and handled during incident response.

3. All contact details from external groups are updated and distributed to the NCERT member responding to the incident response.

4. The NCERT Supervisor must monitor all communication activities.

5. All communication with external groups or third parties are recorded and documented accordingly.

6. All records of communication are reviewed at regular intervals to evaluate the procedures and processes in conducting communication with other parties outside NCERT.

6.8 Review Procedure

Introduction

The review stage is an important process to ensure that the established incident response system of CSB is working efficiently and effectively. It is also a chance for NCERT to analyze and evaluate lessons that can be learned from the data gathered and collected including the related responses and associated decisions undertaken during initial and post incident activities. The review stage provides the avenue to also monitor all unresolved including resolved cases to evaluate the recommendations provided during incident response.

Scope

This section will cover the review procedures that are conducted by the NCERT as part of the objective for continuous improvement.

Control Objectives

1. Post incident reviews are conducted to determine the efficiency of the processes and procedures established for the NCERT.

2. Outputs of the reviews and its corresponding results are used as an input for refining the processes and procedures of NCERT.

3. Review outputs are documented for evidentiary purposes.

a. Review Procedures

1. All records and documented activities for incident responses are reviewed at regular intervals.

2. A monthly meeting with the NCERT is scheduled to review all post incident reports that were resolved immediately during the initial response are summarized for discussion.

3. For incident reports requiring longer period of investigation, schedules for meeting are conducted with more frequency to ensure that all response activities are monitored and reviewed.

4. All post incident reports that took longer time to be resolved are reviewed and evaluated further to gather lessons to be learned:

i. Develop knowledge database of best practices from lessons learned;

ii. Develop knowledge database for research and development;

iii. Consolidate the knowledge database for latest techniques, approaches and methods for incident response;

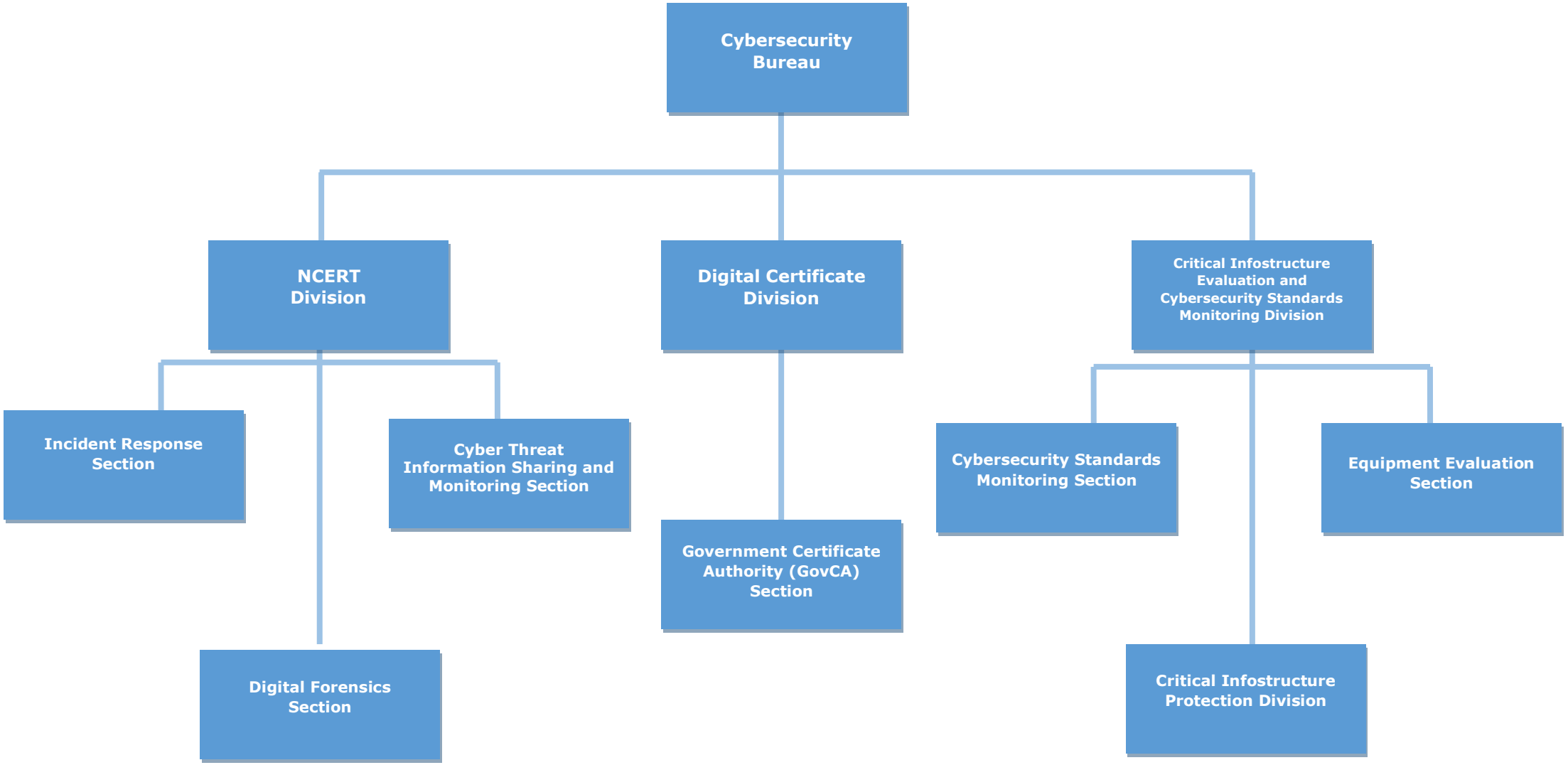
iv. All communication and coordination activities must be reviewed to improve the procedures and processes when communicating outside NCERT;

v. Results of review meetings and discussions are reviewed during the next schedule of meeting; and

vi. All reviews are documented and records are submitted to CSB.

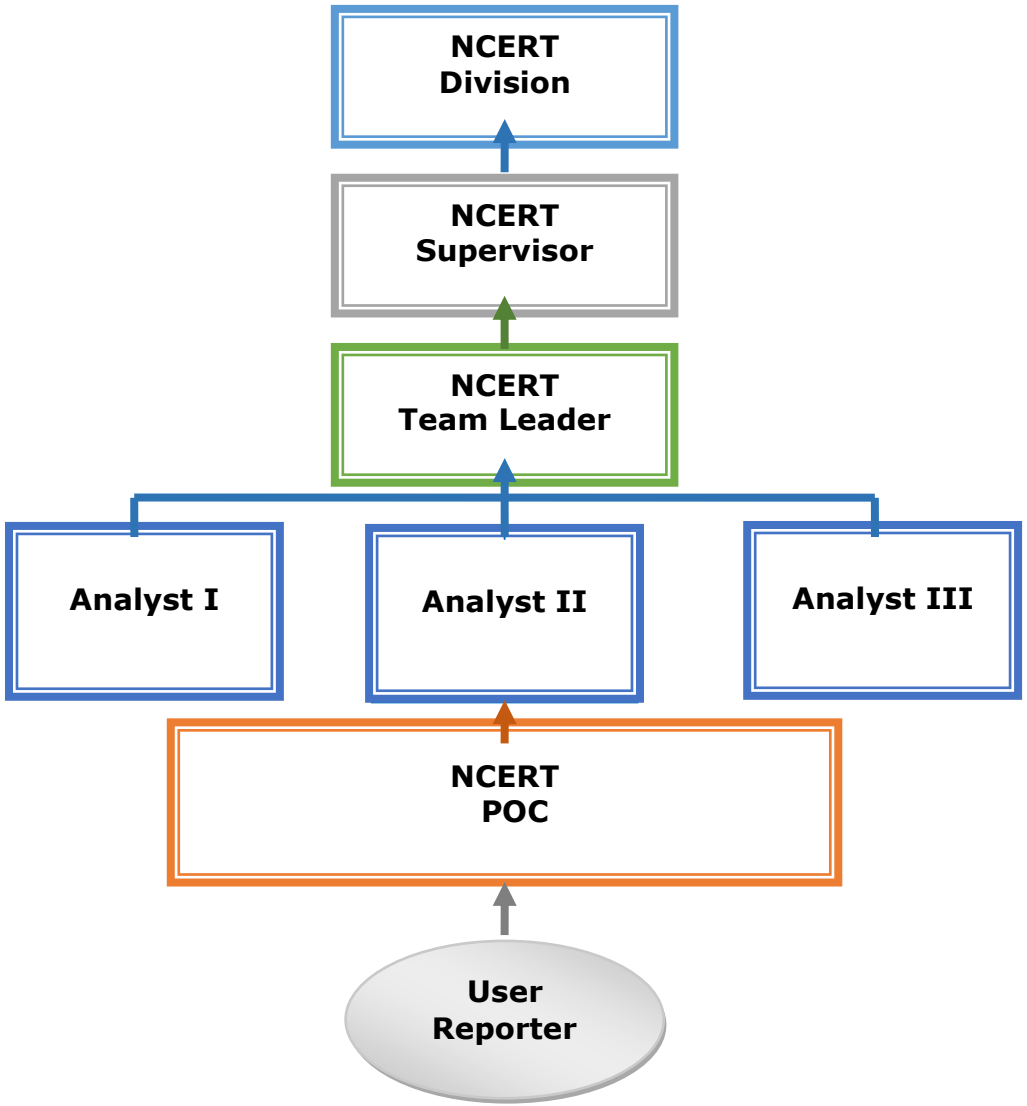
ANNEX A

Organizational Structure



ANNEX B

NCERT Structure



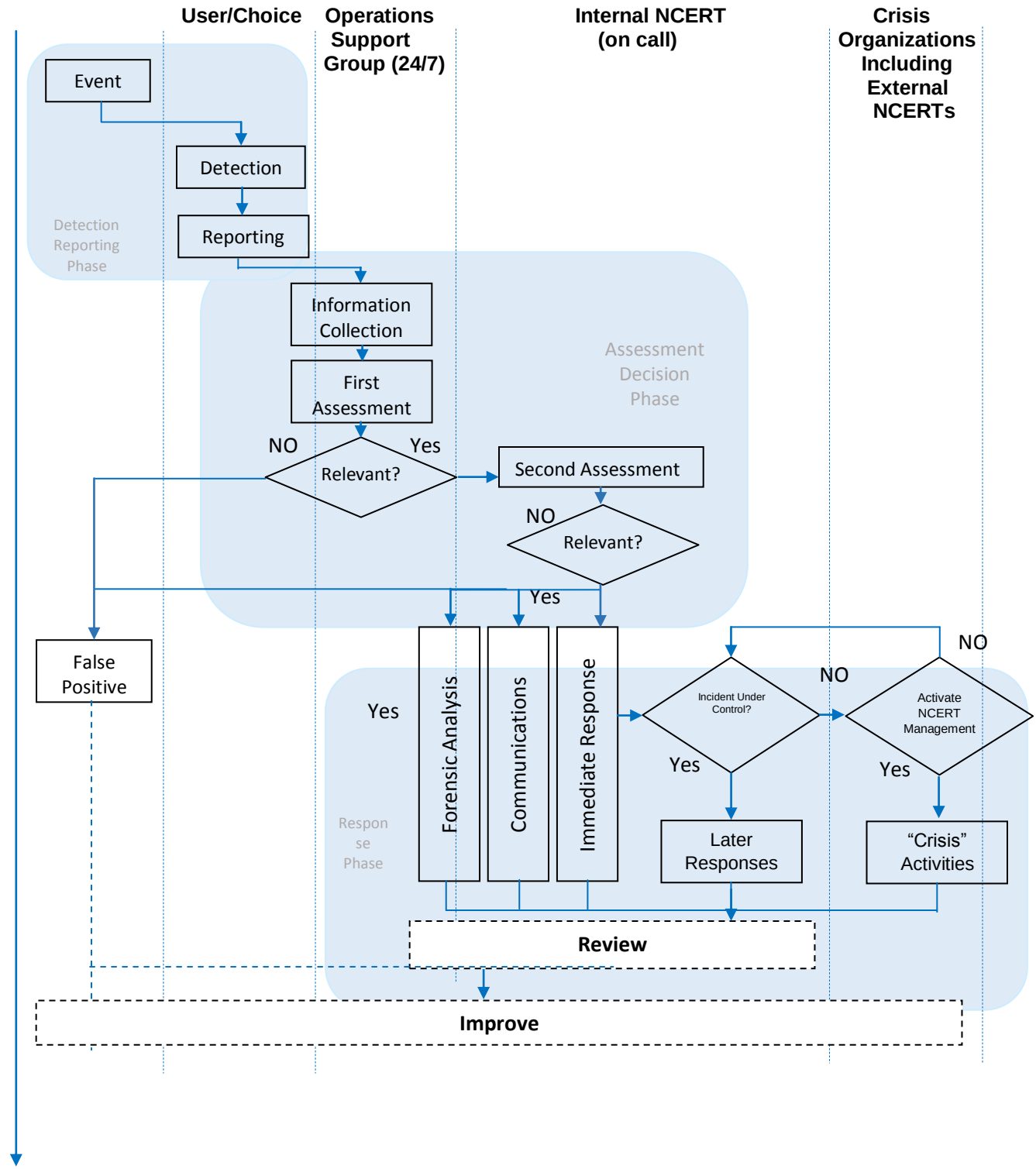
ANNEX C

Skills and Competency Framework

Level	Position	Set Skills	Competency	Mastery or Expertise
1	POC	Computer literate, communication skills, encoding, probing techniques, basic knowledge on OS, active listening skills, listening comprehension skills	Customer service management, critical thinking skills, analytical thinking skills, general administrative skills, multi-tasking ability	Conflict resolution management skills, public relations and communications skills
2	Analyst and Team Leader	Advance computer knowledge, technical and report writing, interpersonal and intrapersonal skills, advance probing technique, time and task management	Leadership skills, supervisory and management skills, planning and execution skills, basic project management skills, ability to conduct forensic based on existing standards, problem solving and decision making skills, high degree in mathematical and logical thinking ability, team motivation ability	Advance digital forensic investigation, wide range knowledge on various types of hardware platform, coaching and mentoring skills, training skills, mastery on computer forensic best practices and industry standard methodologies for acquiring and handling of digital evidence, advance technical understanding of digital forensic principles and techniques, solid knowledge on laws and regulation related to ICT and computer
3	Supervisor	Digital forensics skills, advance computer forensic hardware and computer knowledge, MS Windows, Unix-like or mobile phone operating systems, negotiating skills with decision makers and executives, extensive knowledge on laws and regulation related to ICT and computer	Leadership skills, mentoring and coaching skills, training skills, conflict resolution management skills, team building development, planning skills, supervisory and managerial skills, advance project management skills, problem solving and decision making skills, mathematically inclined with logical thinking ability	Superior knowledge of computer forensic best practices and industry standard methodologies for acquiring and handling of digital evidence, superior technical understanding of digital forensic principles and techniques

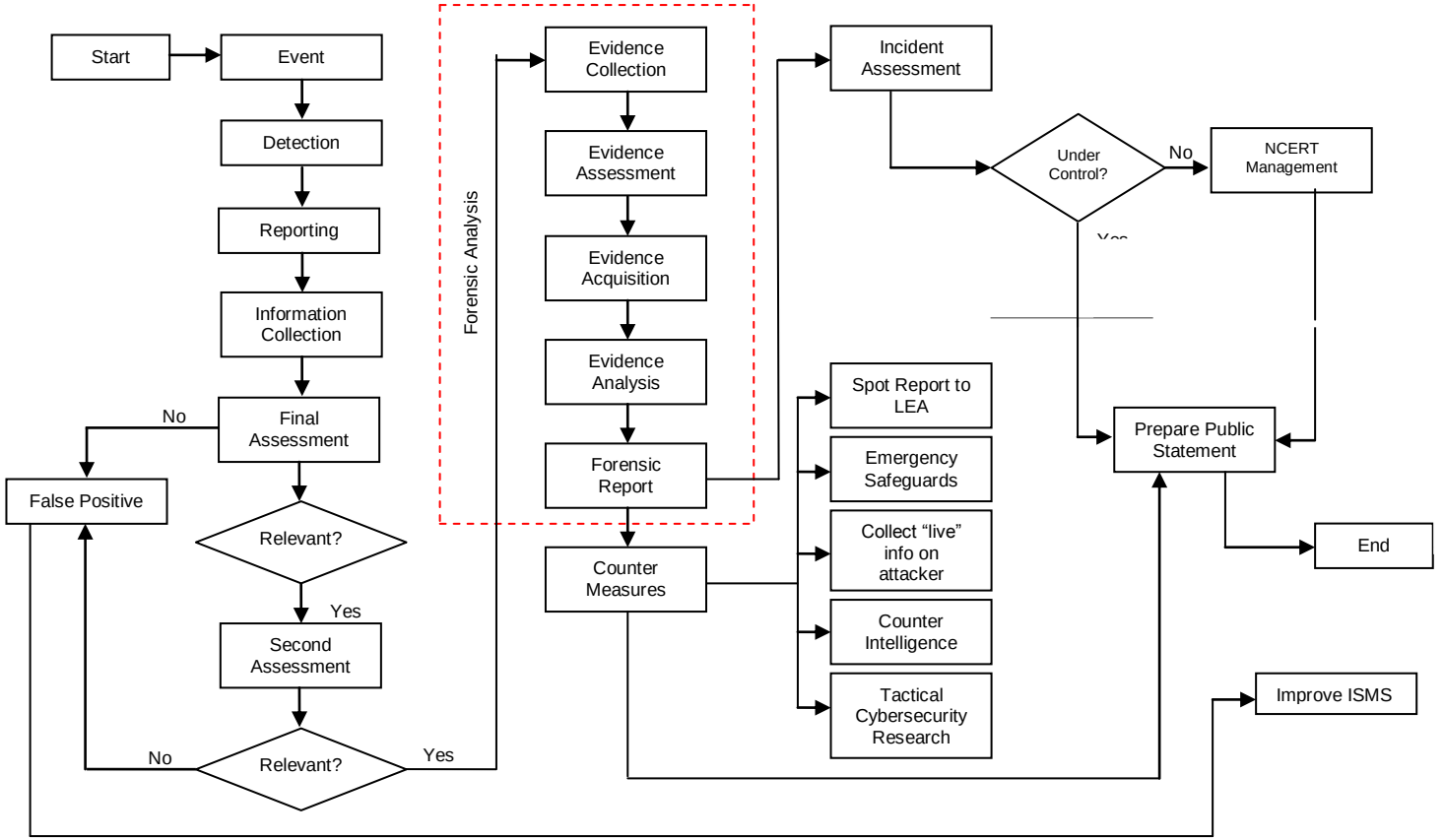
ANNEX D

National Computer Emergency Response Team (NCERT) Key Processes



ANNEX E

Flowchart for Incident Handling Responses



Date Event Reported		POC Person	
Case Number		Related Case No.	

Initial Assessment Form (IAF1)

Reporting Person Details

Name _____

Organization _____

Address _____

Primary Contact No. _____ Email Address _____

Secondary Contact No. _____ Alternate Email Address _____

Information Security Event Description

Description of the Event:

What Occurred

- ☐ Loss of service
- ☐ Loss of equipment
- ☐ Loss of facility
- ☐ System malfunction
- ☐ System overload
- ☐ Software malfunction
- ☐ Intrusion attempt
- ☐ Human error
- ☐ Bad application design
- ☐ Compliance violations
- ☐ Access violations
- ☐ Physical/security breach
- ☐ Uncontrolled system changes
- ☐ Others (please specify)

How Occurred

- ☐ Theft
- ☐ Fraud
- ☐ Sabotage/Physical Damage
- ☐ Malicious Code
- ☐ Hacking/Logical Infiltration
- ☐ Misuse of Resources
- ☐ Hardware Failure
- ☐ Software Failure
- ☐ Hardware Maintenance Error
- ☐ Communication Failure
- ☐ Fire
- ☐ Flood
- ☐ Design Error
- ☐ User Error
- ☐ Operations Error
- ☐ Software Maintenance Error
- ☐ Third Party Services
- ☐ Others (please specify)_____

Why Occurred

- ☐ Deliberate or Intentional
- ☐ Actual Attack
- ☐ Accidental
- ☐ Others _____

Provide brief summary:

Components Affected

- ☐ People/Organization
- ☐ Hardware
- ☐ Software
- ☐ Resources
- ☐ Information
- ☐ Services
- ☐ Legal or Regulatory Obligations
- ☐ Others (please specify)_____

Adverse Business Impacts

- ☐ Financial Loss
- ☐ Personal Information
- ☐ Loss of Goodwill
- ☐ Loss of Reputation
- ☐ Legal and Regulatory
- ☐ Obligations
- ☐ Management and Business Operations
- ☐ Disruption to Business Operations
- ☐ Commercial and Economic Interests
- ☐ Others (please specify)_____

Vulnerabilities Identified

- ☐ Information
- ☐ People
- ☐ Physical (e.g. hardware)
- ☐ People
- ☐ Software (e.g. computer program
- ☐ Reputation and Image
- ☐ Processes, procedures policies, guidelines
- ☐ Services
- ☐ Others (please specify)_____

Information Security Event Details

Date the Event Occurred		Time the Event Occurred	
Date the Event was Discovered		Time the Event was Discovered	
Date the Event was Reported		Time the Event was Reported	

Is the Event Over? ☐ Yes ☐ No

If yes, Specify How Long the Event has lasted in

☐ Days _____ ☐ Hours _____ ☐ Minutes _____

Provide brief summary:

POC	Name of Person Receiving 1st Assessment Report: (Time and Date must be included in the received stamp)

Date Event Reported		POC Person	
Case Number		Related Case No.	

Final Assessment Form (FAF1)
Reporting Person Details

Name _____

Organization _____

Address _____

Primary Contact No. _____ Email Address _____

Secondary Contact No. _____ Alternate Email Address _____

Information Security Event Description

Description of the Event:

What Occurred

- ☐ Loss of service
- ☐ Loss of equipment
- ☐ Loss of facility
- ☐ System malfunction
- ☐ System overload
- ☐ Software malfunction
- ☐ Intrusion attempt
- ☐ Human error
- ☐ Bad application design
- ☐ Compliance violations
- ☐ Access violations
- ☐ Physical/security breach
- ☐ Uncontrolled system changes
- ☐ Others (please specify)

How Occurred

- ☐ Theft
- ☐ Fraud
- ☐ Sabotage/Physical Damage
- ☐ Malicious Code
- ☐ Hacking/Logical Infiltration
- ☐ Misuse of Resources
- ☐ Hardware Failure
- ☐ Software Failure
- ☐ Hardware Maintenance Error
- ☐ Communication Failure
- ☐ Fire
- ☐ Flood
- ☐ Design Error
- ☐ User Error
- ☐ Operations Error
- ☐ Software Maintenance Error
- ☐ Third Party Services
- ☐ Others (please specify)_____

Why Occurred

- ☐ Deliberate or Intentional
- ☐ Actual Attack
- ☐ Accidental
- ☐ Others _____

Provide brief summary:

- ☐ People/Organization
- ☐ Hardware
- ☐ Software
- ☐ Resources
- ☐ Information
- ☐ Services
- ☐ Legal or Regulatory Obligations
- ☐ Others (please specify)_____

Adverse Business Impacts

- ☐ Financial Loss
- ☐ Personal Information
- ☐ Loss of Goodwill
- ☐ Loss of Reputation
- ☐ Legal and Regulatory
- ☐ Obligations
- ☐ Management and Business Operations
- ☐ Disruption to Business Operations
- ☐ Commercial and Economic Interests
- ☐ Others (please specify)_____

Vulnerabilities Identified

- ☐ Information
- ☐ People
- ☐ Physical (e.g. hardware)
- ☐ People
- ☐ Software (e.g. computer program
- ☐ Reputation and Image
- ☐ Processes, procedures policies, guidelines
- ☐ Services
- ☐ Others (please specify)_____

Information Security Event Details

Date the Event Occurred		Time the Event Occurred	
Date the Event was Discovered		Time the Event was Discovered	
Date the Event was Reported		Time the Event was Reported	

Is the Event Over? ☐ Yes ☐ No

If yes, Specify How Long the Event has lasted in

☐ Days _____ ☐ Hours _____ ☐ Minutes _____

Provide brief summary:

POC	Name of Person Receiving 2nd Assessment Report: (Time and Date must be included in the received stamp)

TYPE OF INFORMATION SECURITY INCIDENT

☐ Actual ☐ Attempted ☐ Suspected

Threat Source Occurred at what Level

☐ Organizational ☐ Level Process ☐ Level Information System Level

Type of Threat Event ☐ Adversarial ☐ Non Adversarial

Assets Affected

(Provide descriptions of the assets affected by or related to the incident including serial, license, version numbers where relevant)

Information/Data .....

Hardware .....

Software .....

Communications .....

Documentation .....

Adverse Business Impact/Effect of Incident

(Provide descriptions of the assets affected by or related to the incident including serial, license, version numbers where relevant)

		Value
Breach of Confidentiality	☐	.....
Breach of Integrity	☐	.....
Breach of Availability	☐	.....
Breach of Non-Repudiation	☐	.....
Destruction	☐	.....

Additional Notes:

INCIDENT RESOLUTION

Incident Investigation Commenced Date .....

Incident Investigator(s) Name(s) .....

Incident End Date .....

Impact End Date .....

Incident Investigation Completion Date .....

Reference and Location of Investigation Report .....

Person(s)/Perpetrators Involved

Person (PE)	☐	Accident (AC)	☐
Organized Group (GR)	☐	No Perpetrator (NP)	☐
Legally Established Organization/Institution (OI)	☐		

Modus Operandi of Perpetrator

Actual or Perceived Motivation

Criminal/Financial Gain (CG)	☐	Revenge (RE)	☐
Political Terrorism (PT)	☐	Other (OM)	☐
Pastime/Hacking (PH)	☐	Specify: _____	

Actions Taken to Resolve Incident

(e.g. no action, in-house action, internal investigation, external investigation by. And other actions)	Brief Summary of Actions Taken to Resolve Incident

Actions Planned to Resolve Incident

(e.g. no action, in-house action, internal investigation, external investigation by. And other actions)	Brief Summary of Actions Taken to Resolve Incident

Actions Outstanding

(e.g. investigation is still required by other personnel)	Brief Summary of Actions Taken to Resolve Incident

CONCLUSION

☐ Major	☐ Minor
Indicate any other conclusion:	Indicate any other conclusion:

Individuals/Entities Notified

This detail to be completed by the relevant person with information security responsilbilities

Information Security	☐	Manager CERT Manager	☐
Site Manager	☐	Information Systems Manager	☐
Report Originator	☐	Report Originator's Manager	☐
Law Enforcement	☐	Other	☐

☐ PNP ☐ NBI ☐ DND

(e.g. Help Desk, Human Resources, Management, Internal Audi, Regulatory Body, External CERT) Please specify: _____

Escalation Classification

☐ For Escalation ☐ For De-Escalation

Current Status of Incident

☐ Open/Unresolved ☐ Close/Resolved

Involved Individuals

Originator		Reviewer		Reviewer	
Signature		Signature		Signature	
Name		Name		Name	
Role		Role		Role	
Date		Date		Date	

Originator		Reviewer		Reviewer	
Signature		Signature		Signature	
Name		Name		Name	
Role		Role		Role	
Date		Date		Date	

Additional Notes:

Case #	Related Case #	Date	Name of Person Requesting Change	Changes Made	Reason for Changes	Approved by	Status

Forensic Image Chain of Custody

Case #: _____ Related Case #: _____ Page ___ of Page ___

Hard Drive/Computer Information

Item #:	Description	
Manufacturer	Model #:	Serial #:

Image Details

Date/Time Image Created:	Created by:	Method Used:	Image Name:	HASH:	Drive Used to Store Image:

Chain of Custody

Tracking No.	Date/Time	From	To	Reason
	Date	Name of Organization	Name of Organization	
	Time	Signature	Signature	
	Date	Name of Organization	Name of Organization	
	Time	Signature	Signature	
	Date	Name of Organization	Name of Organization	
	Time	Signature	Signature	
	Date	Name of Organization	Name of Organization	
	Time	Signature	Signature	
	Date	Name of Organization	Name of Organization	
	Time	Signature	Signature	