Forum of Incident Response and Security Teams

(FIRST)

OPERATIONAL FRAMEWORK

September 11, 1992 Table of Contents

Forum of Incident Response and Security Teams
(FIRST)
Operational Framework

INTRODUCTION

The Forum of Incident Response and Security Teams (FIRST) consists of a network of individual computer security incident response teams that work together voluntarily to deal with computer security problems and their prevention. These teams represent government, law enforcement, academia, the private sector, and other organizations with justifiable interest as determined by the Steering Committee.   This Framework describes the FIRST, its organization, and basic operational policies.

PURPOSE

The primary purpose of the FIRST is to provide a forum for participating organizations to work together to share current information, solve common problems, and plan future strategies.

GOALS

The goals of the FIRST are:

- fostering cooperation among information technology constituents in the effective prevention, detection, and recovery from computer security incidents;   providing a means for the communication of alert and advisory information on potential threats and emerging incident situations; facilitating the actions and activities of the FIRST members including research, and operational activities; and facilitating the sharing of security-related information, tools, and techniques.

DEFINITIONS

Response Team - an organization whose function is to assist an information technology community or other defined constituency in preventing and handling security-related incidents.   An individual Response Team also takes active steps to raise its constituents' level of awareness of computer security issues and to improve the security of its constituents' information technology resources.

Constituency - a group of users or organizations that is served by a given Response Team and that share specific characteristics, such as a specific organization, computer network, operating system, or other common interest.

FIRST Representative - an individual who is the designated representative of a FIRST Member.   The FIRST Representative may delegate this authority and must notify the Secretariat in writing of the delegation.

FIRST Member - a Response Team which is a member of FIRST.   In this framework, the terms Member and FIRST Member are used interchangeably.

Incident - an event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.

Liaison - an individual or a representative of an organization other than a Response Team that has a legitimate interest in and value to the FIRST.

Secretariat - a FIRST Member or other group designated by 2/3 vote of the Steering Committee to serve as an administrative distribution point for FIRST, to coordinate FIRST meetings and workshops, maintain Member profile information, and provide general guidance to new Members and potential members.

Steering Committee - a group of individuals responsible for general operating policy, procedures, and related matters affecting the FIRST as a whole.

FIRST PARTICIPATION

Types of Participation

There are two types of participants in the FIRST:

> _FIRST Members, and

> _Liaisons.

The selection and responsibilities of each type of participant are described in this framework.

Membership

Initial FIRST Members

The initial Response Teams comprising the FIRST are listed in Appendix A. Additional members shall be accepted as described below.

Nomination & Acceptance Procedures

New participants in the FIRST, either as Members or Liaisons, must be nominated by an existing Member and approved by a 2/3 vote of all members of the Steering Committee.

A proposed new FIRST Member or Liaison must provide the following information in support of its nomination:

> _The name or identification of the group or organization

> _Identification and description of its constituency

> _Reasons for joining the FIRST

> _Benefits to FIRST of nominee's participation

> _Name of FIRST Representative or Liaison point of contact

> _Completion of other appropriate information for the "participant profile"

maintained for each Response team as described in Section H.1 below.

The term of membership is indefinite.

Membership Termination

E.2.3.1 Voluntary Termination - A Member or Liaison may voluntarily resign from the FIRST at any time.

E.2.3.2 Revocation - Participation may be revoked for non-compliance with this FIRST Framework, lack of cooperation, or failure to contribute to the purposes and goals of the FIRST.   Two FIRST Members must propose in writing to the Steering Committee that a participant be dropped from the FIRST.   The participant shall be provided an opportunity for rebuttal prior to a vote by the Steering Committee.   Revocation shall require a 2/3 vote of all members of the Steering Committee.

GENERAL COORDINATION AND ORGANIZATION

The general coordination of FIRST activities will be provided by the Steering Committee, designated committees, and the Secretariat.

Steering Committee

The Steering Committee shall be responsible for general operating policy, procedures, and related matters affecting the FIRST as a whole.

Steering Committee Membership

The initial Steering Committee shall consist of one representative of each of the initial Response Teams listed in Appendix A.   Five of those original Steering Committee members will be chosen at random to serve until the second General Meeting; the remaining members will serve until the first General Meeting.   After the first General Meeting, the Steering Committee shall comprise ten individuals serving two-year terms.

Nomination and Election

Individuals for one-half (5) of the Steering Committee positions shall be elected at each annual General Meeting.   A candidate must be nominated by petition of at least six (6) FIRST Members.   A FIRST Member may vote for no more than the number of open positions. The five candidates receiving the most votes shall become members of the Steering Committee.   Ties shall be broken by random selection.

Chair

The Steering Committee shall elect from its membership a chair to serve a term of one year.

A person may not serve as Chair for more than two consecutive one-year terms.

Vacancies

A vacancy shall occur when a Steering Committee member resigns or is removed.   A Steering Committee member may be removed for cause by a unanimous vote of the remaining Steering Committee Members.   The Steering Committee Chair shall nominate a person to complete the remaining term.   The nominee must be approved by a 2/3 vote of the remaining Steering Committee.

Standing and Ad Hoc Committees

The Steering Committee will establish, as necessary, standing and ad hoc committees.   The Steering Committee shall appoint the membership and chair of such committees and shall determine their operating procedures.

FIRST Secretariat

A Secretariat shall be designated by the Steering Committee. The responsibilities of the Secretariat shall include coordinating FIRST meetings and workshops, maintaining FIRST Member profile information, keeping informed of individual FIRST Member and Liaison activities, and serving as an administrative distribution point for the FIRST. The Secretariat shall also provide general guidance to new Members, potential members, and Liaisons.

MEETINGS

General Meetings

The FIRST shall hold a General Meeting annually.   FIRST Members are expected to be represented.   Each Response Team shall be represented by its FIRST Representative.   The business of the annual General Meeting shall include the election of the Steering Committee members and may include any other matter affecting the FIRST. Minutes of meetings shall be taken and distributed to all Members, Steering Committee members, and Liaisons.

Conduct of General Meeting

The chair of the Steering Committee shall preside at the General Meeting.   All business shall be conducted in accordance with Roberts' Rules of Order, latest revision.

Voting and Conduct of Meetings

Each FIRST Representative shall have one vote.   A quorum shall be a number of FIRST Representatives equalling one-half the number of FIRST Members plus one (1).   All matters except as described elsewhere in this Operational Framework shall be decided by a simple majority vote of the quorum.

Steering Committee Meetings

The Steering Committee shall meet at least semi-annually.   A quorum shall comprise at least six (6) members.   All matters shall be decided by a two-thirds (2/3) affirmative vote of the quorum except as described elsewhere in this Operational Framework.   Minutes of meetings shall be taken and distributed to all Members and Liaisons.

Working Meetings

The Steering Committee may call working meetings to deal with specific subjects.

Participation may be limited due to the nature of the subject being addressed.

PARTICIPANT REQUIREMENTS & RESPONSIBILITIES

Each Member and Liaison is expected to adhere to the provisions of this Framework, meet certain operational requirements, and fulfill certain responsibilities to the other participants.

Participant Profile

Each participant must provide and maintain a profile of itself describing the constituency and technical expertise provided.

Communications Support

Each Member must provide the operational and communications support capabilities as determined by the Steering Committee.

FIRST Representative

Each Member must designate a FIRST Representative and alternate. All official correspondence will be addressed as designated by the FIRST Representative.

FUNDING

Member Participation

All participants must provide their own funding and support for their participation in FIRST activities.

Additional Funding and Support

The Steering Committee or Secretariat may accept funding or other support for FIRST activities.

OPERATIONAL ACTIVITIES & POLICIES

FIRST Communications

All FIRST information and communications shall be provided security protection appropriate to the nature and sensitivity of the information involved.

Handling and Dissemination of Information

All FIRST participants must adhere to the dissemination constraints specified by the originating source. Only the originator may relax any dissemination constraints. Information that has no specific dissemination instructions may not be disseminated further.

Non-Disclosure Agreements

If a FIRST Member obtains information subject to a non-disclosure agreement, no rights to that information may be assumed by other Members.

Public Release of Information

Each FIRST Member should have an established procedure for interaction with the press in accordance with the FIRST Member's constituency requirements.   Where possible and appropriate, notices and other information should be distributed to the FIRST in advance of public release.   In all situations, an individual Response Team is responsible to its constituents first and may work with the press if necessary to reach its constituency.   Individual Members may not speak for other FIRST Members nor the FIRST as a whole.   The Steering Committee may authorize the Secretariat or a FIRST Member to speak for the FIRST.

Representation

The people working voluntarily as members of the FIRST are working as employees of their parent organizations. The FIRST is an organization strictly for the purposes as enumerated in Section B, and is not an official organization or legal entity.

Language

All business of the FIRST shall be conducted in English.

AMENDMENTS

Amendments to this Framework must be approved by a 2/3 vote of all the FIRST Representatives.   The proposed amendment must be on the agenda at the annual General Meeting to be considered for acceptance.   This Framework shall be reviewed on an annual basis by the Steering Committee and appropriate changes proposed to the FIRST membership.

DISSOLUTION

The FIRST may be dissolved when approved by a 2/3 vote of all the FIRST Representatives.

APPENDIX A - INITIAL MEMBERS

The following organizations shall be initial members of the FIRST:

Air Force Computer Emergency Response Team (AFCERT)

Computer Emergency Response Team/Coordination Center (CERT/CC)

Defense Communication Agency/Defense Data Network (DCA/DDN)

Department of Army Response Team

Department of Energy's Computer Incident Advisory Capability, Lawrence

Livermore National Laboratory (DOE's CIAC)

Goddard Space Flight Center

NASA Ames Research Center Computer Network Security Response Team

(NASA ARC CNSRT)

        NASA Space Physics Analysis Network (SPAN CERT)

        Naval Computer Incident Response Team (NAVCIRT)

        National Institute of Standards and Technology Computer Security Resource
and Response Center (CSRC)

        SPAN-France