FEDERAL COMPUTER INCIDENT RESPONSE CAPABILITY (FEDCIRC)

The need for an incident handling capability that crosses agency boundaries has never been greater. Almost all federal agencies are now connected to the Internet and exchange information regularly. The large number of Internet-related incidents that have occurred in the past year, along with the increase and complexity of threats, requires agencies to take seriously their incident handling capability. The Office of Management and Budget has emphasized this need in OMB Circular A-130, Appendix III, by requiring agencies to be able to respond in a manner that both protects their own information and helps to protect the information of others who might be affected by the incident. The private sector is undergoing the same rapid growth in network dependency as the federal community and is in need of the same incident handling support. Several private-sector organizations have foreseen this need and have begun to offer incident handling services.

In answer to the need for a U.S. Government-wide incident response capability to assist federal civilian agencies, the National Institute of Standards and Technology (NIST) initiated the Federal Computer Incident Response Capability (FedCIRC) Program. Initially funded by the Government Information Technology Services (GITS) Innovation Fund Committee, FedCIRC assists federal civilian agencies in their incident handling efforts by providing proactive and reactive computer security-related services. This CSL Bulletin describes the FedCIRC Program.

FedCIRC History

In 1989, NIST and several other organizations sought to develop a group to facilitate sharing computer security, vulnerability, and threat information. The group evolved into the Forum of Incident Response and Security Teams (FIRST). FIRST is now an international coalition which brings together a variety of computer security incident response teams from government, commercial, and academic organizations. Currently FIRST has more than 55 incident response teams participating as members. While developing FIRST, NIST recognized the need for a centralized group to handle computer security-related incidents for the federal civilian community. Until now, that need was not fully addressed primarily due to funding and control issues. The funding required could not be placed solely on one agency.=20 Additionally, a neutral organization was needed to house the capability. Accordingly, NIST conceived and proposed the idea of FedCIRC to GITS. GITS approved the proposal and on October 21, 1996, FedCIRC became operational.

The mission of FedCIRC is to develop a self-sustaining incident response capability that meets the needs of the federal civilian agencies. It is envisioned that the needs of the agencies will evolve as agencies begin to develop their own incident handling capabilities. FedCIRC will be flexible in its mission to meet those ever-changing needs. Critical to the success of FedCIRC is a continued awareness of what the federal civilian agencies are

doing on their own and where they need FedCIRC assistance.=20
FedCIRC combines the experience and expertise of NIST's Computer Security Division, the Defense Advanced Research Project Agency's CERT(SM) Coordination Center (CERT/CC), and the Department of Energy's Computer Incident Advisory Capability (CIAC) to provide agencies with cost-reimbursable, direct technical assistance and incident handling support.=20

Operations
The FedCIRC operations team is comprised of individuals from three distinct organizations (NIST, CERT/CC, and CIAC) that operate in concert. Each organization has its prime roles and responsibilities and also contributes to the overall project. NIST subcontracts the operational incident handling capability to CERT/CC and CIAC. NIST is responsible for operational management and for facilitating the development of incident handling standards and guidelines by utilizing the threat and vulnerability data collected by FedCIRC. The vulnerability information will also be used in the analysis and testing of software and other products. =20

Services
FedCIRC provides six primary services to federal civilian agencies. The amount of service depends on the subscription level to which an agency or major operating unit subscribes. The services are: incident handling information, incident response and hotline support, annual FedCIRC incident handling conference, semi-annual "state of the threat" subscriber meetings, information security evaluation, and assistance in establishing an on-site incident response capability. These services are briefly described in the following paragraphs.

Incident Handling Information
The incident handling information is the foundation of FedCIRC.=20
The availability of the incident response hotline support and the collection, analysis, and publication of threat, vulnerability, and other security-related data can only be accomplished if the underlying infrastructure is in place. The infrastructure consists of the following activities:

=07 alert creation;
=07 interaction with other incident handling organizations, law enforcement, and vendors;
=07 threat and trend analysis;
=07 hotline availability;
=07 data tracking;
=07 vulnerability analysis;
=07 report generation;
=07 database maintenance;
=07 guidance documents (e.g., best practices);
=07 web site maintenance; and
=07 technology watch.

FedCIRC subscribers will receive by e-mail a Quarterly Summary Report which contains sanitized data and statistics about types

of incidents, trends, and information on new tools and guidance on preventing and handling incidents. The Quarterly Summary Report is available to the public and will include aggregate data on number of calls, number of incidents handled, type of incidents handled, type of systems attacked, and effects of incidents. It will not contain names of sites or FedCIRC subscribers. =20

FedCIRC will maintain a public web site to provide access to a repository of tools and to give example practices. The following outline presents some of the topics to be covered on the FedCIRC web site.

=07 What is FedCIRC? (a description of FedCIRC services and how to take advantage of them);
=07 e-mail list services;
=07 alerts and advisories;
=07 useful security tools;
=07 repository of useful computer security-related documents such as best practices;
=07 virus information;
=07 pointers to FIRST (Forum of Incident Response and Security Teams);
=07 pointers to other security servers;
=07 communication with FedCIRC; and
=07 training opportunities.

A set of FedCIRC security alerts, modeled after the CIAC Bulletins and the CERT Advisories, will be made available to FedCIRC members as events require. These alerts will include a description of the vulnerability or problem, the platform(s), operating system(s) affected, the impact of the vulnerability problem, and patches and work-arounds, if available. The alerts will reflect the combined expertise and perspectives of the nation's most experienced incident response teams.

Incident Response and Hotline Support
Emergency technical assistance in response to computer security incidents is provided 24 hours per day, seven days a week. A "help desk" provides assistance during "normal business hours" (8:30 a.m. to 9:00 p.m. EST/EDT). Assistance is provided via telephone, e-mail, and pager hotline.=20

Incident response support ranges from providing agencies with direct technical support to handle computer security incidents or providing backup support to agency response teams dealing with large and complex incidents, to only providing agency response teams with information on threats, vulnerabilities, and countermeasures that allow agency teams to effectively deal with incidents on their own.=20

Many activities are required to provide an incident response.=20
Some sample activities that provide this support include:

=07 problem analysis: analyze the problem, determine the magnitude of the threat, and provide technical assistance in identifying and closing vulnerabilities;

=07 technical advice: issue advisories to the agencies warning of the problem and describing countermeasures;

=07 technical advice: provide guidelines on implementing vulnerability patches and other security controls;

=07 assistance: facilitate the interaction of victims and relevant law enforcement agencies in reporting security incidents involving violations of the law;

=07 assistance: coordinate with other security organizations including the Forum of Incident Response and Security Teams (FIRST);

=07 assistance: work with vendors to provide critical security patches and work-arounds; and

=07 vulnerability analysis: perform vulnerability analysis to identify a vulnerability's root cause to mitigate or prevent potential problems before they occur.

The types of operating systems FedCIRC will handle include:=20
UNIX, VMS, MVS, DOS, Windows, Mac, NT, VM, and MPE-XE. The types of protocols covered include: TCP/IP, IPX, Ethernet, LAT, DECnet, Token Ring, and FDDI.

Annual FedCIRC Incident Handling Conference
An annual conference on the current state of security threats and security improvement practices will be held in the Washington, D.C. area. The conference will provide an opportunity for federal agencies to share lessons learned from security incidents and the results of security improvement efforts. The annual conference will be a two-day event addressing countermeasures identified as reducing the current risks to federal information systems. Some of the proposed agenda topics or tracks for the annual conference are:

=07 status of the FedCIRC effort;
=07 updates from various FedCIRC members, e.g., successes, lessons learned;
=07 sessions on forming and sustaining an organic incident response capability;
=07 session on incident escalation and when to contact the FedCIRC hotline; and
=07 trade show exhibit space for vendors.

Semi-Annual "State of the Threat" Subscriber Meetings
In a given year, two subscriber meetings will be conducted.=20
Meeting agendas will consist of two and a half days of briefings on current incident trends, recent vulnerabilities, latest

viruses, and concentrated training. Detailed descriptions, impacts, fixes, and work-arounds will be disseminated at subscriber meetings. FedCIRC subscribers will share related experiences, current practices, policies, and procedures during these meetings. General topics to be covered during the state-of-the-threat meetings will include:

=07 an overview of FedCIRC and its goals;
=07 a description of FedCIRC services;
=07 a review of FedCIRC expectations placed on subscriber agencies;
=07 current incident trends;
=07 recent vulnerabilities -- descriptions, impacts and fixes or work-arounds;
=07 current intruder tools -- descriptions, usage, countermeasures;
=07 recent viruses and identification of anti-virus packages to combat them or interim protection methods;
=07 a review of existing viruses and vulnerabilities that continue to be exploited;
=07 presentations by FedCIRC members describing related experiences and current practices;
=07 open discussion and questions and answers about relevant policies and procedures; and
=07 technical training seminars, including:

- Internet Security for System and Network Administrators,
- Connecting to the Internet Securely,
- LAN Security for Desktop Systems - Novell, Windows 95/NT, and
- Virus Detection, Eradication, and Prevention.

The training that is provided during the semi-annual subscriber meetings will evolve as required to address current computer and information risks.=20

Information Security Evaluation
An information security evaluation (ISE) of a single agency program will be conducted. The program to be evaluated will be identified prior to signing an interagency agreement. The evaluation will be performed over a four-month time frame and will be tailored to the subscriber's needs. The ISE assessment includes a review of selected components of the agency's network policy, infrastructure, and network topology. The assessment identifies high-leverage improvement opportunities and the most serious network vulnerabilities.

Recommendations on improving the security of the program will be presented in a report. A one-day training session designed for the agency and addressing the report's recommendations will be presented on-site for all network and security administrators.=20

Assistance in Establishing an On-Site Incident Response Capability

Mentoring and hands-on training at CERT/CC and/or CIAC will be conducted for a maximum of five students. Subscriber agencies are responsible for students' travel and accommodations.=20
Training will be tailored to the needs of the subscriber. The training consists of working with incident handling specialists to answer hotline calls, handle incidents, and prepare alerts.=20
All the issues, such as dealing with the press, law enforcement, security and network experts, and vendors, will be explored through first-hand experience.=20

This training covers topics such as:

=07 volunteer Incident Response Capability (IRC) option;
=07 incident escalation to FedCIRC;
=07 defining a budget and sustaining it over fiscal years;
=07 space, equipment and personnel;
=07 operational issues - incident handling procedures, physical, and electronic security;
=07 press issues;
=07 confidential versus public information;
=07 developing technical documents and standard replies;
=07 developing a FAQ (Frequently Asked Question);
=07 training constituency on reporting incidents, encryption, and other computer-related security topics;
=07 types of incidents;
=07 types of responses;
=07 importance of reference numbers;
=07 staffing requirements; and
=07 information requests.

Funding
FedCIRC is only funded for the first year through the Government Information Technology Services (GITS) Innovation Fund. At the end of the first year, the GITS committee will make a determination whether to provide an additional half year of funding. The option for additional funding is based on agency buy-in and on what has been accomplished through FedCIRC=FEs first year. The plan to convert the FedCIRC pilot project into a self-sustaining program is through agency subscriptions. Agencies subscribe to FedCIRC Incident Response Handling Services based on several yearly subscription rates below. The services provided under each subscription rate can be tailored to the agency's individual needs.

Platinum -- $250,000.
Gold -- $110,000.
Silver -- $ 50,000.

Contact Information
For more detailed information about FedCIRC, contact Marianne Swanson or Fran Nielsen at 301-975-4369 or e-mail at fedcirc.info@nist.gov. The FedCIRC web site can be reach at the URL: http://csrc.nist.gov/fedcirc. If incident handling assistance is needed, please contact the FedCIRC Hotline at 412-268-6321 or e-mail at fedcirc@nist.gov.