FCC
Computer Security Incident Response Guide

December 2001

Federal Communications Commission
Office of the Managing Director
Information Technology Center
Computer Security Program

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 PURPOSE 1
1.2 BACKGROUND 1
1.3 SCOPE 3
2 ROLES AND RESPONSIBILITIES 3
2.1 USERS 3
2.2 MANAGERS 3
2.3 SYSTEM ADMINISTRATORS 3
2.4 AUCTIONS OPERATIONS GROUP 4
2.5 COMPUTER INCIDENT RESPONSE TEAM (CIRT) 4
2.6 COMPUTER SECURITY OFFICER (CSO) 4
2.7 OFFICE OF INSPECTOR GENERAL (OIG) 4
2.8 OFFICE OF MEDIA RELATIONS (OMR) 5
3 THREAT ENVIRONMENT 5
3.1 INTERNAL AND EXTERNAL THREAT 5
3.2 MALICIOUS CODE ATTACKS 5
3.2.1 Virus Incidents 6
3.2.2 Macro Viruses 6
3.2.3 Worms 6
3.2.4 Trojan Horses 7
3.2.5 Cracking Utilities 7
3.3 CRACKER/HACKER ATTACKS 8
3.4 TECHNICAL VULNERABILITIES 9
4 PROCEDURES FOR RESPONDING TO INCIDENTS 10
4.1 PREPARATION 11
4.1.1 Baseline Protection 11
4.1.2 Planning and Guidance 11
4.1.3 Training 12
4.2 IDENTIFICATION 12
4.2.1 Determine the Symptoms 12
4.2.2 Identify the Nature of the Incident 14
4.2.3 Identify the Evidence 14
4.2.4 Protecting the Evidence 14
4.2.5 Report the Events 15
4.3 CONTAINMENT 15
4.3.1 Maintain a Low Profile 16

4.3.2 Avoid Potentially Compromised Code......................16
4.3.3 Back up the System 16
4.3.4 Change Passwords 17
4.4 ERADICATION 17
4.4.1 Determine the Cause and Symptoms 17
4.4.2 Improve Defenses 17
4.4.3 Perform Vulnerability Analysis 17
4.5 RECOVERY...18
4.5.1 Determine the Course of Action 18
4.5.2 Monitor and Validate System 18
4.6 FOLLOW-UP 18
4.6.1 Document Response Quality to Incident....................18
4.6.2 Document Incident Costs...19
4.6.3 Preparing a Report..19
4.6.4 Revising Policies and Procedures 19

5 LEGAL ISSUES 19

6 CONCLUSION..20

APPENDIX A: GLOSSARY A-1
APPENDIX B: REFERENCES...B-1

ATTACHMENT: FCC COMPUTER SYSTEM INCIDENT RESPONSE FORM...1-1

1 INTRODUCTION

1.1 Purpose

The purpose of this computer security incident response guide is to provide general guidance to Federal Communications Commission (FCC) staff - both technical and managerial - to: enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information.

It is also a guide to sharing information with other organizations — internally within the FCC, and externally with other information security and law enforcement organizations, as well as a guide for pursuing appropriate legal action, consistent with Department of Justice guidance.

The challenge of incident response is to be able to bring a large number of FCC staff with divergent skills together quickly and effectively in a crisis situation. To prepare for this challenge, the FCC has developed specific policies, procedures, and guidelines. This document provides a general overview of the preparations the FCC has made to respond to computer security incidents and some specific help for system users when they first become aware of an incident. This guide, coupled with the FCC's security awareness training, addresses the OMB A-130 requirement "to share information concerning common vulnerabilities and threats."

1.2 Background

OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, (updated in 1996) significantly changed the way federal agencies are required to protect their computer assets. OMB A-130 divides computer assets into two broad categories: General Support Systems and Major Applications.

Among the requirements for securing these computer assets is an incident response process for general support systems[1], the purpose of which is to deal effectively with a security incident should one occur.

OMB A-130 requires an incident response capability to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities, threats, and corrective actions taken. Information sharing with other organizations should be consistent with National Institute of Standards and Technology (NIST), and should assist the Commission in pursuing appropriate legal action, consistent with Department of Justice guidance.

Responding to computer security incidents is generally not a simple matter. Effective incident response requires a high level of technical knowledge, communication, responsibility, and coordination among FCC technical staff that must respond to these incidents. However, the end user, who generally does not have the required skills for effective incident response, is sometimes the first person to become aware of an incident. Therefore, the explicit emphasis in OMB A-130 is on providing help to the end user in both incident response and in end-user awareness of system threats and vulnerabilities. Furthermore, the legal knowledge required in assessing the ramifications of remedial actions generally only resides in the FCC's Office of General Counsel (OGC), the Information Technology Center (ITC) and Office of Inspector General (OIG). Moreover, the program knowledge required to assess the damage caused by a security incident and restore the integrity of the system is generally concentrated in the system owners and administrators who work daily with the system and its data.

Appendix A provides a glossary of terms commonly used in incident handling and computer security. Appendix B provides a list of references used in this document.

[1] Although OMB A-130 does not explicitly require an incident response capability for major applications, logical extension of the intent of A-130 indicates that these incident response guidelines should apply for each major application in which a security incident could reasonably occur.

1.3 Scope

The guidance contained in this document is directed at the technical staff, e.g., system administrators, ITC personnel, and the Auctions Operations Group. However, this guidance is applicable to all FCC employees and contractors (collectively known as FCC users), and others who process, store, transmit, or have access to IT information and infrastructure computing resources in the Commission. This guidance is applicable to all FCC information and infrastructure computing resources, at all levels of sensitivity, whether owned and operated by the FCC or operated on behalf of the FCC.

2 ROLES AND RESPONSIBILITIES

Each of the FCC's staff members, from end users of the FCC's network resources to the Commissioner's office, has responsibilities related to the security of the FCC's computing systems.

2.1 Users

Despite advances in automated intrusion detection systems, computer users may be the first to discover an intrusion. Both end and system users need to be vigilant for unusual system behavior, which may indicate a security incident in progress.

In addition to their incident reporting responsibilities, system users may at some point be responsible for reporting incidents (e.g., a virus infection, a system compromise, or a denial of service incident, which is detected by resident software on the system user's workstation) to the Computer Resource Center (Help Desk).

2.2 Managers

Managers ensure that their employees are aware of the reporting procedures and the security policies in place to protect FCC information systems, employees and property. They are responsible for reporting security incidents to the ITC and for notifying the Computer Security Officer (CSO).

2.3 System Administrators

System Administrators, familiar with FCC systems, may often be the first to discover a security incident. Like managers, system administrators are responsible for immediately reporting these incidents to the CSO. Additionally, they may be called upon to help determine and implement a solution, when applicable.

2.4 Auctions Operations Group

The Auctions Operations Group is responsible for running the intrusion detection packages that serve as an early warning system for any hacker/cracker or disruption of service attacks against all Auctions systems.

2.5 Computer Incident Response Team (CIRT)

The CSO has established the FCC CIRT. The CIRT is the Commission's response team designed to assist on behalf of the FCC Chief Information Officer (CIO) in handling security incidents. Team's responsibilities include discovery of, and response to, activities, which might otherwise interrupt the day-to-day operations of the FCC computer infrastructure, formalizing reporting of incidents.

Furthermore, the CIRT is established to formalize reporting of incidents and disseminating incident information with ITC staff and the user community.

2.6 Computer Security Officer (CSO)

The CSO is responsible for coordinating computer security efforts within the FCC. It is also the CSO's responsibility to advise the CIO and other system managers in the event of a serious security incident, and coordinate the response with senior management, the OIG, and other law enforcement authorities.

2.7 Office of Inspector General (OIG)

The OIG provides law enforcement authority and investigative support to any incident handling initiatives. If criminal activity is suspected, OIG must be notified immediately. As determined by the OIG, other law enforcement support may be called in to assist in the investigation of an incident.

2.8 Office of Media Relations (OMR)

The FCC's OMR is responsible for answering questions from the public regarding activities within the FCC. When a computer security-related incident occurs, the OMR may disseminate information, if needed, to the public. FCC personnel are not authorized to disseminate information related to a computer security incident to the public (including the press), but should work to provide such information to the CSO who will coordinate with OMR.

3 THREAT ENVIRONMENT

Although computer security incidents may take many forms and involve many devious means, there are certain types of attacks which occur more frequently than others. Knowing what these types of attacks are and how the FCC counters them will help the FCC staff be best prepared to react and report all related information to the CSO.

3.1 Internal and External Threat

Internal Threat. An internal threat is any instance of a user misusing resources, running malicious code or attempting to gain unauthorized access to an application. Examples include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. More significant internal threats may include an otherwise authorized system administrator who performs unauthorized actions on a system.

External Threat. An external threat is any instance of an unauthorized person attempting to gain access to systems or cause a disruption of service. Examples include disruption/denial of service attacks, mail spamming, and execution of malicious code that destroy data or corrupt a system.

3.2 Malicious Code Attacks

Malicious code is typically written to mask its presence thus it is often difficult to detect. Self-replicating malicious code, such as viruses and worms, can replicate so rapidly that containment can become an especially difficult problem. Dealing with malicious code attacks requires special considerations.

3.2.1 Virus Incidents

A virus is self-replicating code that operates and spreads by modifying executable files. Viruses are often user-initiated and would pose virtually no threat if every user always followed sound procedures. In general, users should not execute attachments without first scanning for infection. E-mail executables tend to carry infectious virus coding.

FCC Response. The FCC provides all users with training concerning how viruses work and the procedures that limit the spread of viruses. The FCC has anti-virus tools in place, including a virus scanner on each desktop PC that checks every file opened as well as a network scanner.

The FCC maintains a known good copy of anti-virus software on a write-protected CD-ROM. The FCC will immediately discontinue using any computer infected by a virus.

Leave the infected computer on and call the Computer Resource Center (CRC). Do not attempt to eradicate the virus and/or restore the system without guidance from the CRC.

3.2.2 Macro Viruses

Macro viruses are a type of virus that utilizes an application's own macro programming language to distribute themselves (e.g., in MS Word or MS Excel).

FCC Response. Because macro viruses infect document files rather than programs, the FCC has extended its virus protection to include the examination of all files using the latest commercial anti-virus application(s). Users will receive instructions on how to turn on macro protection in their MS Office applications.

3.2.3 Worms

A Worm is self-replicating code that is self-contained, (i.e., capable of operating without modifying any software). Worms are best noticed by looking at system processes. If an unfamiliar process (usually with an unknown name) is running and is consuming a large proportion of a system's processing capacity, the system may have been attacked using a worm. Worms also sometimes write unusual messages to users' displays to indicate their presence. Messages from unknown users that ask the user to copy an electronic mail message to a file may also propagate worms. Worms generally propagate themselves over networks and can spread very quickly.

FCC Response. If any FCC staff member observes the symptoms of a worm, he or she must inform the CRC immediately. Use the attached Virus Report form (Attachment 2)

Prompt killing of any rogue processes created by the worm code will minimize the potential for damage. If the worm is a network-based worm, i.e., uses a network to spread itself, ITC will disconnect any workstations or client machines from the network.

3.2.4 Trojan Horses

Trojan horse programs are hostile programs masquerading as valid programs or utilities. Most malicious code is really a Trojan horse program in one way or another. Trojan horse programs are often designed to trick users into copying and executing them.

3.2.5 Cracking Utilities

Cracking utilities are programs sometimes planted in systems by attackers for a variety of purposes, such as elevating privileges, obtaining passwords, disguising the attackers’ presence and so forth. They can be used from outside the system to gather information as well as to launch attacks against the target system.

3.3 Cracker/Hacker Attacks[2]

Crackers and hackers are users who attempt to obtain unauthorized access to remote systems. Until recently, crackers and hackers used virtually the same surreptitious methods to intrude. The average hacker still sits at a terminal entering commands, waits to see what happens, and then enters more commands. Now, most cracking attacks are automated and take only a few seconds, which makes identifying and responding to them more difficult. Crackers now generally use "cracking utilities," (described above) which usually differ from conventional malicious code attacks in that most cracking utilities do not disrupt systems or destroy code. Cracking utilities are typically "a means to an end," such as obtaining administrative-level access, modifying audit logs, etc.

Modem dial-ins are a favorite way to crack or hack systems.

FCC Response. It is FCC policy is that all modem lines are to be set as dial-out or made available on stand-alone PCs only.

Indications that a cracker or hacker may have compromised a system include the following symptoms:

- changes to directories and files;
- a displayed last time of login that was not the actual time of last login;
- finding that someone else is logged into an individual's account from another terminal; or
- inability to login to an account (often because someone has changed the password).

[2] The principal distinction between these two types of intruders is that 1) "crackers" intrude with the intent of attacking specific systems, or inserting, deleting, or modifying specific data; 2) "hackers" intrude for the thrill. Hackers may cause damage, but it is as an afterthought, not premeditated.

FCC Response. If these or other suspicious symptoms are noticed, ITC Technical Support should be notified immediately. Use the attached Incident Response form (Attachment).

If an attacker is caught in the act of obtaining unauthorized access, the FCC follows procedures dependent on the nature of the attack.

- If the attacker has obtained administrative-level access, is deleting or changing user files, or has access to a machine that contains sensitive data, the attack poses a serious threat. In this case, the CIRT locks the attacker out of this system by aborting the processes the attacker has created.
- If the cracker does not obtain administrative-level access and does not appear to be damaging or disrupting a system, the CIRT *may* elect to allow the attacker to continue so as to collect the evidence necessary to catch and/or prosecute the attacker.

A critical stage in cracker/hacker attacks is eradication. Because crackers so frequently use cracking utilities, it is important to ensure that no cracking scripts remain on the system once the cracker's attack has ceased.

Another critical component of responding to cracker/hacker attacks is handling evidence that is gathered. System log printouts, copies of malicious code discovered in systems, backup tapes, referring to chains of custody and entries recorded in logbooks may conceivably be used as evidence against perpetrators. (See paragraph 4.2.4).

FCC Response. If a system user finds evidence of such cracking artifacts, the FCC CIRT will make copies of the artifacts and forward them to the CSO and OIG for further examination. The CIRT will work to restore any file permissions and configuration settings that the attacker may have changed to their normal value. Resolving cracker/hacker attacks is risky, unless one possesses the technical skills, programs, and equipment necessary, which is specifically why the CIRT has been established.

3.4 Technical Vulnerabilities

As opposed to an internal or external threat, a technical vulnerability is a “hole” or weakness in an information system or components (e.g., system security procedures, hardware design, and internal controls) that could be exploited to violate system security. Most of the currently known technical vulnerabilities in applications and operating systems have been discovered during development testing, user acceptance testing, Certification and Accreditation, Security and Test and Evaluation, and OIG Audits.

FCC Response. If a user discovers a technical vulnerability that could be used to subvert system or network security, he or she should immediately document that vulnerability and forward it to the CSO and the associated system administrator, using the attached Incident Report form. This document should record the following information:

(1) describe the vulnerability;

(2) describe the circumstances under which the vulnerability was discovered;

(3) describe the specific impact of the weakness or design deficiency; and

(4) indicate whether or not the applicable vendor has been notified.

After documenting the vulnerability, the information should be brought immediately to the attention of the CSO, even if the normal chain of command has to be circumvented. **Do not** send vulnerability reports over the network, or share vulnerability information with anyone outside of official channels. The CSO will coordinate the efforts to resolve the vulnerability with the system administrator, CIO and OIG.

4 PROCEDURES FOR RESPONDING TO INCIDENTS

The FCC defines six stages of response when servicing a computer security incident: *preparation, identification, containment, eradication, recovery,* and *follow-up*. Knowing about each stage facilitates responding more methodically and efficiently, and helps key staff understand the process of responding so that they can deal with unexpected aspects of incidents they face. The following paragraph defines the six stages of response.

4.1 Preparation

The FCC considers being prepared to respond *before* an incident occurs to be one of the most critical facets of incident handling. This advance preparation avoids disorganized and confused response to incidents. The FCC's preparation also limits the potential for damage by ensuring that response plans are familiar to all staff, thus making coordination easier.

4.1.1 Baseline Protection

The FCC has installed baseline protection on all systems and networks. All computing components have a first-line level of defense to keep incidents from spreading quickly from system to system. The FCC local area network (LAN) servers have access controls set so that no one except the LAN administrator(s) can write to system executables.

As is always the best practice, the FCC system administrators maintain compliance with CERT notices, bulletins, and incident and vulnerability notes to ensure that all appropriate defensives are in place before an incident occurs.

The FCC has obtained potentially useful tools in advance to avoid the potentially damaging delays that can occur when starting to procure such tools after an incident has happened. Examples include virus detection and eradication tools.

The FCC has implemented an intrusion detection system (IDS) and monitors and responds to alerts.

4.1.2 Planning and Guidance

The FCC has established a Computer Incidence Response Team[3] (CIRT). Assigned system administrators will be available during a critical incident involving one or more essential systems. In case administrator-level access is needed by someone other than the assigned system administrator, passwords used to obtain administrative-level access to every system and LAN in the FCC have been recorded in separate envelopes and placed in the ITC data media safe.

[3] Computer Incident Response Team procedures are described in *FCC Computer Incident Response Team (FCC CIRT)* Guide, July 2002.

The FCC has planned for emergency communications needs. Should an incident adversely affect regular communication channels, the FCC has prepared lists of personnel to be contacted during incidents, including home phone numbers and primary and secondary FAX numbers, cell phones and pager numbers. See the FCC Computer Incident Response Team (FCC CIRT), June 1998 document.

The FCC has created written incident response guidance, made it widely available, and distributed it to all levels of staff. This written guidance is structured to help the average system administrator respond to unexpected events that may be symptoms of computer security incidents.

4.1.3 Training

Training has been provided to the appropriate CIRT personnel. Training focuses on how to respond to incidents. CIRT members are also required to participate in periodic mock incidents in which written incident response procedures are followed for simulated incidents.

4.2 Identification

The FCC's approach to the Identification Stage involves 1) validating the incident, 2) if an incident has occurred, identify its nature, 3) identifying and protecting the evidence, and 4) logging and reporting the event or incident. When a staff member notices a suspicious anomaly in data, a system, or the network, he or she begins the FCC's identification process.

4.2.1 Determine the Symptoms

Determining whether or not an anomaly is symptomatic of an incident is difficult since most often apparent symptoms of a security incident are something else, (e.g., errors in system configuration, application bugs, hardware failures, user error, etc.).

Typical symptoms of computer security incidents include any or all of the following:

(a) A system alarm or similar indication from an intrusion detection tool;

(b) Suspicious entries in system or network accounting (e.g., a UNIX user obtains root access without going through the normal sequence);

(c) Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which no entries whatsoever appear);

(d) Unsuccessful logon attempts;

(e) Unexplained, new user accounts;

(f) Unexplained new files or unfamiliar file names;

(g) Unexplained modifications to file lengths and/or dates, especially in system executable files;

(h) Unexplained attempts to write to system files or changes in system files;

(i) Unexplained modification or deletion of data;

(j) Denial/disruption of service or inability of one or more users to login to an account;

(k) System crashes;

(l) Poor system performance;

(m) Operation of a program or sniffer device to capture network traffic;

(n) "Door knob rattling" (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts);

(o) Unusual time of usage (remember, more computer security incidents occur during non-working hours than any other time);

(p) An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user; and

(q) Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

4.2.2 Identify the Nature of the Incident

Although no single symptom conclusively shows that a computer security incident is taking place, observing one or more of these symptoms prompts the observer to investigate events more closely. System Administrators who encounter one or more of these symptoms should work with the CSO and designated ITC points of contact to determine exactly what has occurred. The FCC will validate security incidents on a case by case basis.

If the incident involves criminal activity or possible criminal activity, the CSO and CIO will make a determination and, based on the outcome, will notify the FCC OIG, the FBI and the national Infrastructure Protection Center (NIPC).

4.2.3 Identify the Evidence

In order to protect the evidence, number, date and sign notes and printouts. Seal disks with original, unaltered, complete logs in a safe, or copy the entire log to an alternate location and secure appropriately. When turning over evidence to the CSO ensure every item is signed for and detailed, factoring in the chain of command.

4.2.4 Protecting the Evidence

The chain of custody for all evidence must be preserved. Documentation will be provided that indicates the sequence of individuals who have handled the evidence and the sequence of locations where the evidence has been stored. Dates and times must be specified as well. There must not be any lapses in time or date. The hand-off of evidence must be documented as well.

The integrity of this information must be checked and provable in the anticipation that it may be challenged. This can be done by preserving the evidence on tamper-resistant media (e.g., CD-R), or generating cryptographic hash or checksum, (e.g., SHA-1, MD5 or CRC32).

The FCC obtains a full backup of the system in which suspicious events have been observed as soon as a computer security-related incident has been declared. Since perpetrators of computer crimes are becoming increasingly proficient in quickly destroying evidence of their illegal activity, be aware that, unless evidence is immediately captured by making a full backup, this evidence may be destroyed before it can be examined. This backup will provide a basis for comparison later to determine if any additional unauthorized activity has occurred.

4.2.5 Report the Events

If a computer-based incident is detected, it must be reported immediately to the CSO. In particular, each system owner must know how and when to contact the CSO. The incident report form attached to this guide should be used to gather information and report on the suspected incident.

The CSO has the responsibility to report incident information to senior management in a timely fashion. In addition, the CSO must report to the CIO promptly in the event of a serious breach of security. If there is evidence of criminal activity, the CIO will direct the CSO to notify the FCC OIG.

CAUTION: No FCC staff member, except the designated FCC spokesperson (and the FBI, if involved) has authority to discuss any security incident with any person outside the FCC

The FCC system and network audit logs provide sufficient information to facilitate deciding whether or not unauthorized activity has occurred. As soon as the CSO and the respective system owners decide that a serious computer security incident has occurred that has wider ramifications, they will notify the OIG and federal authorities.

4.3 Containment

The FCC's immediate objective for the Containment Stage is to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator.

The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. The CSO and system owner will work within appropriate investigative organization(s) to determine if sensitive data should be left on the system or copied to media and taken off-line. Similarly, a decision may be made to move critical computing services to another system on another network where there is considerably less chance of interruption.

A decision on the operational status of the compromised system itself will be made. Whether this system be 1) shut down entirely, 2) disconnected from the network, or 3) be allowed to continue to run in its normal operational status (so that any activity on the system can be monitored) will depend on the risk to assets threatened by the incident.

In the case of a simple virus incident, the FCC CIRT will move quickly to eradicate any viruses without shutting the infected system down. If the system is highly sensitive or information and/or critical programs may be at risk, the FCC will generally shut down the system down (or at least temporarily isolate it from the network). If there is a reasonable chance that letting a system continue to run as normal without risking serious damage, disruption, or compromise of data can identify a perpetrator, the FCC may continue operations under close monitoring.

4.3.1 Maintain a Low Profile

If a network-based attack is detected, the FCC must be careful not to tip off the intruder.

Avoid looking for the attacker with obvious methods - if hackers detect an attempt to locate them they may delete systems.

Maintain standard procedures - continue to use the FCC intrusion detection systems.

4.3.2 Avoid Potentially Compromised Code

It is not advisable to log in as root or administrator and then start typing commands to a system suspected of being compromised. For example, avoid using ftp to download tools from another site. If possible, record the fingerprint of critical binaries for the organization's core operation systems.

4.3.3 Back up the System

Back up the affected system to a new unused media. Do a backup as soon as there are indications that a security incident has occurred. Making a full backup immediately captures evidence that may be destroyed before having a chance to look at it. Make two backups; one to keep sealed as evidence and one to use a source of additional backups.

4.3.4 Change Passwords

Immediately change the passwords on all affected systems. Passwords should be changed on comprised systems and on all systems that regularly interact with the compromised systems and notify all affected staff of the password change. If a sniffer device is detected or suspected, passwords may have been compromised on all systems on the LAN. It is important that users change to a unique password that is not being used on any other computer system.

4.4 Eradication

The next priority, after containing the damage from a computer security incident, is to remove the cause of the incident. In the case of a virus incident, the FCC will remove the virus from all systems and media (e.g., floppy disks, backup media) by using one or more proven commercial virus eradication applications. The FCC recognizes that many intrusions leave benign or malignant artifacts that can be hard to locate. Therefore, the FCC will concentrate on the eradication of 1) malignant artifacts (e.g., Trojan horses) and 2) benign artifacts, only if they present a serious enough risk to justify the cost.

4.4.1 Determine the Cause and Symptoms

Use information gathered during the containment phase and collect additional information. If a single attack method cannot be determined list and rank the possibilities.

4.4.2 Improve Defenses

Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's functions to a more secure operating system.

4.4.3 Perform Vulnerability Analysis

Use FCC’s RealSecure or a comparable product as a vulnerability analysis tool to scan for vulnerable systems that are connected to affected systems.

4.5 Recovery

The FCC defines recovery as restoring a system to its normal mission status.

4.5.1 Determine the Course of Action

In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not adversely affect the FCC's computer or data resources. In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restoration operation from backup tapes or full implementation of the FCC's disaster recovery plans.

4.5.2 Monitor and Validate System

First, determine the integrity of the backup itself by attempting to read its data. Once the system has been restored from backup, verify that the operation was successful and that system is back to its normal operating condition. Second, run the system through its normal tasks monitoring it closely by a combination of network loggers and system log files. Monitor the system closely for potential "back doors" that may have escaped detection.

4.6 Follow-up

The FCC realizes that devoting further resources to an incident after the Recovery Stage is not always cost effective. However, the FCC also realizes that following up on an incident after Recovery helps to improve incident handling procedures.

4.6.1 Document Response Quality to Incident

Obtain answers to the following questions to assess how well the agency responded to the incident:

- Was there sufficient preparation for the incident?
- Did detection occur promptly or, if not, why not?
- Could additional tools have helped the detection and eradication process?

- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?

4.6.2 Document Incident Costs

Work internally to determine the staff time required to address with the incident (including time necessary to restore system). This leads to the following cost analyses:

- How much is the associated monetary cost?
- How much did the incident disrupt ongoing operations?
- Was any data irrecoverably lost, and, if so, what was the value of the data?
- Was any hardware damaged, and, if so, what was the cost?

Deriving a financial cost associated with an incident can help in prosecuting, as well as serve as a basis to justify future budget requests for security efforts.

4.6.3 Preparing a Report

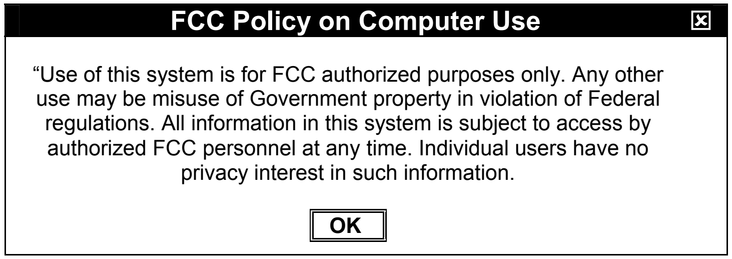
Depending on the type of incident, the FCC will prepare a report, including "lessons learned" and cost analyses described above. Those portions of the report that can be used to further the FCC's staff awareness (without endangering the FCC's security mechanisms) will be appropriately distributed and/or used in training. See the report form attached to this guide.

4.6.4 Revising Policies and Procedures

The FCC realizes that developing effective computer security policies and procedures often requires revising those efforts in light of experience. Therefore, "lessons learned" from each incident are used to review the FCC's computer security measures.

5 LEGAL ISSUES

To avoid compromising the ability to prosecute perpetrators of computer crime, the FCC system displays a warning banner visible to all users who attempt to login to the system. The warning banner (a copy is shown below) advises users that the system is a U.S. Government system and only official use is allowed. Any unauthorized use may result in criminal prosecution. The login banner also includes a statement to the effect that use of a system constitutes voluntary consent to have one's computing-related activity monitored.



FCC Policy on Computer Use

"Use of this system is for FCC authorized purposes only. Any other use may be misuse of Government property in violation of Federal regulations. All information in this system is subject to access by authorized FCC personnel at any time. Individual users have no privacy interest in such information.

6 CONCLUSION

These guidelines stress two fundamental principles related to incident response.

The first principle is the importance of following well-defined and systematic procedures for responding to computer security-related incidents. The six stages of the FCC's incident response procedures (preparation, detection, containment, eradication, recovery, and follow-up) provide a sound basis for securing the FCC's computer resources. They also serve as a foundation for developing custom procedures tailored to specific operational environments. The only effective way to respond to incidents is to use a structured methodology.

The second principle is that unless conducted systematically, incident response efforts are of little value. Coordination of effort is a critical facet of incident response. FCC staff members can significantly reduce the staff hours needed to respond to incidents if properly coordinated.

APPENDIX A: GLOSSARY

Anomaly	An unusual or atypical event (in a system or network).
Attack Scanner	A tool used to remotely connect to systems and determine security vulnerabilities that have not been fixed in those systems.
Cracker	A person who obtains or attempts to obtain unauthorized access to computer resources for specific, premeditated crimes. (See also Hacker)
Checksum	Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation.
Code	System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
Cracking Utilities	Programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, disguising the attacker's presence.
Cryptographic	A checksum that is generated using a checksum cryptographic means. It is used to detect accidental or deliberate modification of data.
Disruption of service	(DOS) occurs when an intruder uses malicious code to disrupt computer services, including erasing a critical program, "mail spamming" i.e., flooding a user account with electronic mail, or altering system functionality by installing a Trojan horse program.
Encryption	Using encryption renders information unintelligible in a manner that allows the information to be decrypted into its original

form - the process of transforming plaintext into ciphertext.

Espionage

Espionage is stealing information to subvert the interests of the FCC, the Federal government, or gaining access to a competitor's data to subvert contract procurement regulations.

Event

Any observable occurrence in a computer system or network, e.g., the system boot sequence, port scan, a system crash, or packet flooding within a network. Events sometimes provide an indication that an incident is occurring, although not necessarily.

Firewall

Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets.

Hacker

A person who obtains or attempts to obtain unauthorized access to computer for reasons of thrill or challenge. (See also Cracker)

Hoax:

A hoax occurs when false stories, fictitious incidents or vulnerabilities are spread (e.g., virus warnings that do not exist).

Incident[4]

An incident is defined as any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.

[4] Includes both deliberate attacks and accidental violations, but, for the purposes of these guidelines, the term "incident" does not encompass such events as natural disasters or failures of basic services to the general community (e.g., power outages, loss of telephone service, etc.) unless caused by deliberate act.

Integrity

(1) A sub-goal of computer security which pertains to ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations.

(2) A sub-goal of computer security, which pertains to ensuring that information, retains its original level of accuracy. Data integrity is that attribute of data relating to the preservation of:

(a) its meaning and completeness,

(b) the consistency of its representation(s), and

(c) correspondence to what it represents.

Intrusion

Unauthorized access to a system or network

Malicious code attacks

Include attacks by programs such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity.

Misuse

Misuse occurs when someone uses a computing system for other than official or authorized purposes.

Sniffer

A device or program that captures packets transmitted over a network

Social engineering

"Conning" unsuspecting people into sharing information about computing systems (e.g., passwords) that should not be shared for the sake of security.

Threat

Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system.

Tiger Team

Government and industry - sponsored teams of computer experts who attempt to break down the defenses of computer systems in an effort to uncover, and eventually patch, security holes.

Trojan horse

Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification or destruction of data.

Unauthorized access

Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories and/or by obtaining "super-user" privileges. Unauthorized access also includes access to network data gained by planting an unauthorized "sniffer" program (or some such device) to capture all packets traversing the network at a particular point.

UUOS

UUOS occurs when an intruder gains unauthorized access to data by planting programs such as a Trojan horse. Other examples include: using the network file system (e.g., Novell) to mount the file system of a remote server machine, using the Virtual Memory System (VMS) file access listener to transfer files without authorization, or using the inter-domain access mechanisms to access files and directories in another organization's domain.

Virus

Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Vulnerability

Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

Worm

Independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads.

APPENDIX B: REFERENCES

- Office of the President
  Presidential Decision Directive 63, *Critical Infrastructure Protection*

- National Institute of Standards and Technology
  ITL Bulletin, *Computer Attacks, What They Are and How to Defend Against Them*, May 1999

- National Institute of Standards and Technology
  Special Publication 800-3*, Establishing a Computer Security Incident Response Capability*, May 1991

- Office of Management and Budget
  Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*

- Federal Communications Commission
  Instruction 1479.2, *FCC Computer Security Directive,* October 2, 2001

- Federal Communications Commission
  Computer Incident Response Team (FCC CIRT), June 1998

- SANS Institute
  Computer Security Incident Handling: Step-by-Step, Version 1.5, 1998

- Computer Emergency Response Team website;
  http://www.cert.org

- Federal Incident Response Center website;
  http://www.fedcirc.gov

ATTACHMENT:

FCC COMPUTER SYSTEM INCIDENT REPORT FORM

This report is designed principally for the use of the ITC, the CSO, and the CIRT for the uniform documentation of incidents. In addition, it may be necessary to gather more data for further analysis; documenting these advanced analyses will involve creating ad hoc reports based on the FCC's mission, legal, and policy requirements.

FCC COMPUTER SYSTEM INCIDENT REPORT FORM

This form is based upon the FedCIRC Incident Report Form, which Federal Agencies and Departments are requested to use when reporting an incident. An automated FedCIRC version of this form can be found on line at http://www.fedcirc.gov/reportform.html. For urgent assistance, call the toll free FedCIRC Hotline at (888) 282-0870.

1. Contact Information for this Incident:

Name:	Organization:	Title:
Address:		
Office Phone:	Cell Phone/Pager:	Fax Number:

2. Physical Location of Affected Computer/Network:

(Include building number, room number, and barcode information, if available):

3. Date and Time Incident Occurred:

Date (mm/dd/yy):	Time (hh:mm:ss am/pm/Time Zone):

4. Type of Incident (check all that apply):

□ Intrusion
□ Denial of Service
□ Virus / Malicious Code
□ System Misuse
□ Social Engineering
□ Technical Vulnerability

□ Root Compromise
□ Web Site Defacement
□ User Account Compromise
□ Hoax
□ Network Scanning / Probing
□ Other (Specify):

4a. If a Virus,
Provide the name(s) of the virus(es):
Provide any URL with information specific to this virus:
Provide a synopsis of the incident:
Actions taken to disinfect and prevent further infection:

4b. If a Technical Vulnerability,
Describe the nature and effect of the vulnerability in general terms:
Describe the conditions under which the vulnerability occurred:
Describe the specific impact of the weakness or design deficiency:
Indicate whether or not the applicable vendor has been notified:

5. Information on Affected System:

IP Address:	Computer/Host Name:	Operating System (incl. release number)	Other Applications:
___________	___________	___________	___________
___________	___________	___________	___________
___________	___________	___________	___________

(include hardware/software, version or release numbers):

7. How Many Host(s) are Affected:

□ 1 to 100 □ 100 to 1000 □ More than 1000

8. IP Address of Apparent or Suspected Source:

Source IP address: ___________ ___________ ___________	Other information available:

9. Incident Assessment:

Is this incident a threat to life, limb, or a critical agency service? □Yes □No If yes, please elaborate:

Sensitivity of the data residing on system:

Damage or observations resulting from incident:

10. Information Sharing:

Has the Public Information Officer been notified? □Yes □No	If yes, provide name and date of notification:

Consider with whom this information may be shared outside of the FCC (do not leave blank and check all that apply):

□ NIPC
□ NSIRC (NSA)
□ JTF-CNO (DoD)

□ Other Government Response Teams
□ Other (Specify):
□ **No Sharing is Authorized**

Note: FedCIRC typically shares information with other government entities in a general sanitized form so as not to implicate a specific agency or department. The sharing is for statistical analysis and trend projection. However, any sharing authorized above may include agency specific information for further analytical and/or investigative purposes. Incidents must be reported to FedCIRC and your respective OIG. Reporting to the NIPC is strongly encouraged.

11. Additional Information:

(If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):

Return this Form to: Computer Security Officer, Room 1-A325
445 12th Street, SW, Washington, DC 20554

Form A-XXX
January 2002

Prepared for:
Federal Communications Commission
Office of the Managing Director
Information Technology Center
Computer Security Program
445 12th Street, SW
Washington, D.C. 20554

Prepared by:

IMSI
INTEGRATED MANAGEMENT
SERVICES, INC.

GSA Schedule Contract Number: GS-35F-4640G
Purchase Order Number: PUR01000885