DEPARTMENT OF THE NAVY NAVSO P-5239-19
AUGUST 1996

COMPUTER INCIDENT RESPONSE GUIDEBOOK

MODULE 19

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

NAVSO P05239-19
AUGUST 1996

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Command, Control and Ocean Surveillance Center
In-Service Engineering East Coast Division
Code 423
P.O. Box 190022
North Charleston, SC 29419-9022

Commercial 1-800-304-4636
E-Mail: subscribe@infosec.nosc.mil

Electronic versions of this document may be downloaded via anonymous ftp from infosec.nosc.mil or /http://infosec.nosc.mil/info.html

Stocked: Additional copies of NAVSO P-5239-19 can be obtained from the Navy Aviation Supply Office (Code 1013), 5801 Tabor Avenue, Philadelphia PA 19120-5099, through normal supply channels in accordance with NAVSUP P600 (CD-ROM only), using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8305.

DEPARTMENT OF THE NAVY

NAVSO P-5239-19
AUGUST 1996

FOREWORD

Naval INFOSEC Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Command, Control and Ocean Surveillance Center In-Service Engineering East Coast Division. It consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or receipt of data. Each module will focus on a distinct program element and describes a standard methodology for planning, implementing and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, "Computer Incident Response Guidebook", provides the Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) with guidance and procedures to be used when responding to computer security incidents.

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

COMPUTER INCIDENT RESPONSE GUIDEBOOK

Ref: (a) OPNAV Instruction 3430.26, Implementation Instruction for Information Warfare/Command and Control Warfare (IW/C2W) dated 18 Jan 95
(b) NSTISSP No.5, National Policy for Incident Response and Vulnerability Reporting for National Security Systems dated 30 Aug 93

1. Background

The United States Government is faced with a new and gigantic challenge---that of Information Warfare. U.S. military computers in particular contain information of great value to adversaries of the U.S. and to "information brokers" who sell information they obtain to other governments and organizations. These same computers often support critical computing activities such as command and control, target tracking, logistics, and control of weapons systems (including systems on Naval vessels and aircraft). Many sensitive unclassified DoN systems connect to the MILNET, (a backbone that ties military networks together all over the world) or the Internet (a backbone that ties all types of networks together throughout the world). The likelihood of attempted, unauthorized access to these systems via the MILNET and other access avenues (e.g., modems) is high. Information warfare requires not only adopting reasonable precautions in securing these systems and networks but also responding quickly and efficiently if system and network security defenses are breached.

Unfortunately, responding to computer security incidents is generally not a simple matter. This activity requires technical knowledge, communication and coordination among personnel who respond to the incident. The incidents themselves are becoming increasingly more complex. For example, during Operation Desert Storm and Desert Shield, dozens of U.S. military systems were illegally accessed by perpetrators who were thousands of miles away (see references in the suggested readings at the end of this document). Sophisticated break-in techniques were employed to obtain data about U.S. troop movements, ordinance systems, and logistics.

At the same time, malicious code such as computer viruses continue to infect military computers in epidemic proportions. Security vulnerabilities that can expose systems and networks to unauthorized access and compromise of integrity are being continually discovered. The toll is often great; weeks and even months may be required to re-establish the integrity of a critical military system which has been compromised by a perpetrator of computer crime or malicious code.

Critical data may fall into the hands of our adversaries. Information system security (INFOSEC) is essential to U.S. military interests; and incident response is a major part of INFOSEC. The importance of incident response at the DoD and national level is realized in references (a) and (b).

2. Purpose.

The purpose of this incident response guidebook includes:

a. Helping DoN personnel quickly and efficiently recover from security incidents. These guidelines reflect "lessons learned" from experience in responding to virtually hundreds of incidents. Following the procedures in these guidelines will acquaint you with proven response measures.

b. Minimizing loss or theft of information (classified or unclassified) or disruption of critical computing services when incidents occur.

c. The need to respond systematically. Following the procedures in this document will increase the likelihood that personnel will carry out all necessary steps to correctly handle an incident.

d. Protecting systems. As desirable as it is to place extremely high levels of defenses (e.g., special access controls) on *all* DoN computing resources, doing so is impossible due to cost and other practical constraints. Being able to detect and recover from incidents quickly can in many respects, be considered a protection strategy to supplement system and network protection measures.

e. Protecting personnel. The safety of many DoN personnel depends on computing systems. Following sound incident response procedures minimizes the likelihood that these systems will function improperly or will become inoperable after a security incident occurs.

f. Using resources efficiently. Having both technical and managerial personnel respond to an incident requires a substantial amount of resources. These resources could be devoted to another mission if an incident were to be short lived. Ending the incident as quickly as possible is, therefore, a high priority so that resources can once again be expended on "normal" operations.

g. Dealing properly with legal issues. A plethora of legal issues surrounds the c omputer security arena. For example, the U.S. Department of Justice has declared certain kinds of monitoring techniques illegal. These procedures have been analyzed from a legal viewpoint and can be followed with the assurance that legal statutes are not being violated.

3. **Scope**.

This document applies to all DoN activities processing GENSER classified or sensitive but unclassified information. Activities operating information systems outside the DoN purview, such as the Naval Security Group will follow the incident reporting requirements established by their Commanding Officer.

The guidelines contained herein contain fundamental information about responding to incidents that is intended to be used independently of particular hardware platforms or operating systems. As such, this guidebook contains neither technically detailed information nor an *exhaustive* set of incident response procedures (although technical information *sources* are described in Appendix A to this document). This document is instead intended to provide a quick, practical source of guidance on incident response.

4. **Definitions**.

Although Appendix A of this guidebook provides a glossary of terms, several terms and concepts are particularly critical. These terms are discussed in this section.

a. **Definition of Incident**

The term "incident" refers to an adverse event in a information system and/or network or the threat of the occurrence of such an event. Examples of incidents include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. Other adverse events include floods, fires, electrical outages, and excessive heat that causes system crashes. Adverse events such as natural disasters and power-related disruptions are not, however, within the scope of this guidebook. For the purpose of this guidebook, therefore, the term "incident" refers to an adverse event that is related to INFOSEC.

An "event" is *any* observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring. In reality, events caused by human error (e.g., unintentionally deleting a critical directory and all files contained therein) are the most costly and disruptive. Computer security-related events, however, are attracting an increasing amount of attention within the DoN and the computing community in general because (among other reasons) the unparalleled growth of networking has so greatly exposed systems to the threat of unauthorized remote access and because of the abundance of malicious code available to perpetrators.

b. **Types of Incidents**

The term "incident" encompasses the following general categories of adverse events:

(1) Malicious code attacks. Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can furthermore replicate rapidly, thereby making containment an especially difficult problem.

(2) 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 unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access could also entail access to network data by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point.

(3) Unauthorized utilization of services. It is not absolutely necessary to access another user's account to perpetrate an attack on a system or network. An intruder can access information, plant Trojan horse programs, and so forth by misusing available services. Examples include using the network file system (NFS) to mount the file system of a remote server machine, the VMS file access listener to transfer files without authorization, or inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain.

(4) Disruption of service. Users rely on services provided by network and computing services. Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

(5) Misuse. Misuse occurs when someone uses a computing system for other than official purposes such as when a legitimate user uses a government computer to store personal tax records.

(6) Espionage. Espionage is stealing information to subv ert the interests of a corporation or government. Many of the cases of unauthorized access to U.S. military systems during Operation Desert Storm and Operation Desert Shield were the manifestation of espionage activity against the U.S. Government.

(7) Hoaxes. Hoaxes occur when false information about incidents or vulnerabilities is spread. In early 1995, for example, several users with Internet access distributed information about a virus called the Good Times Virus, even though the virus did not exist.

Note that these categories of incidents are not necessarily mutually exclusive. A saboteur from

a remote country could for example obtain unauthorized access to a DoN system for the purpose of espionage.

5. Organizational Roles.

The purpose of this section is to describe the roles and responsibilities of different organizations and individuals within the DoN INFOSEC organizational hierarchy. Each individual, from data entry personnel using a PC to the CNO or CMC, have responsibilities related to the security of DoN computing systems. It is important, therefore, that all personnel understand their roles and responsibilities in relationship to this organization.

a. Users

Computer users are nearly always most effective in discovering intrusions that occur. Despite advances in automated intrusion detection systems, most computer incidents are detected by the end users, not by centralized technical measures. Users need to be vigilant for unusual system behavior which may indicate a security incident in progress. These indications are described further in Section 6.b.(2). Users are also responsible for reporting incidents according to the procedures contained in Section 6.e.

In addition to their incident reporting responsibilities, users may at some point be responsible for handling minor incidents. A virus infection that is detected by resident software is one such type of incident.

b. Information Systems Security Officer (ISSO)

The ISSO is the individual responsible for operational security within a subset of machines assigned to a particular site or facility. Each organization has at least one ISSO. The ISSO is the first level of interaction for users experiencing security incidents. It is the ISSO's responsibility to co-ordinate incoming information, advise users on handling low-level security incidents, pass information up through the ISSM, and disseminate information downwards as appropriate.

c. Information Systems Security Manager (ISSM)

The ISSM is responsible for coordinating computer security efforts within an organization. The ISSM will pass incoming incident information from the ISSOs to the Fleet Information Warfare Center (FIWC) in a timely fashion. It is also the ISSM's responsibility to advise the Commanding Officer in the event of a serious security incident, and co-ordinate the response with security personnel.

d. **Fleet Information Warfare Center (FIWC)**

FIWC is an operational command tasked to be the Fleet CINC's principal agent for development of IW/C2W tactics, procedures and training, under the operational control of Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), additional duty to CINCPACFLT, CINCUSNAVEUR and CONUSNAVCENT. FIWC is responsible to provide the following protect services to fleet and shore establishments: Computer Incident Response, Vulnerability Analysis and Assistance, and Incident Measurement.

e. **Naval Computer Incident Response Team (NAVCIRT)**

NAVCIRT is a response team designed to assist ISSOs and ISSMs in handling security incidents. NAVCIRT's responsibilities furthermore include guiding the ISSOs and ISSMs in operating secure systems and networks and disseminating incident information.

NAVCIRT has no law enforcement capability or authority. Criminal investigation and prosecution is the Naval Criminal Investigative Service's (NCIS's) responsibility . It is, however, NAVCIRT's responsibility to advise the ISSO/ISSM community concerning preservation of evidence and downstream liability.

It is also NAVCIRT's mission to disseminate security tools to the user community.

f. **Naval Criminal Investigative Service (NCIS)**

The NCIS is responsible for investigating criminal activity involving DoN personnel or facilities. This includes computer trespass, theft, and espionage. The NCIS is primarily concerned with apprehending and prosecuting criminals. If criminal activity is suspected, NCIS should be notified immediately. This service may not, on the other hand, be able to assist in the response or provide more than a cursory investigation if the evidence has not been preserved or if the case does not prove worth the investment in prosecution (e.g., because the incident is extremely minor).

g. **Public Affairs Office (PAO)**

The PAO is responsible for answering questions from the public regarding military activities. When a security-related incident occurs, it is also PAO's responsibility to disseminate appropriate information to the public. Navy personnel may not disseminate incident-related information to the public (including the press), but should instead work through their chain of command to provide any needed information to the PAO.

6. Procedures for Responding to Incidents

Recommended procedures for responding to incidents are covered in this section.

a. **Rationale for Structured Procedures**

Following pre-defined, structured procedures is a critical component of responding to incidents. Reasons include:

(1) Organization. Someone who is responding to an incident will be more effective if that person's responses are organized. It is easy to forget a critical step or to repeat a step unnecessarily unless one follows organized procedures.

(2) Comprehension. Structured procedures can be read and understood more accurately and rapidly than can non-structured procedures.

(3) Retention. Structured procedures can be learned more easily than can non-structured procedures.

(4) Evolution. Structured procedures are more conducive to improvement and incorporation of "lessons learned."

b. **Stages of Responding to Incidents**

There are at least six identifiable stages of response to an INFOSEC incident. They include preparation, identification, containment, eradication, recovery and follow-up. Knowing about each stage facilitates responding more methodically (and thus efficiently), and also helps users understand the process of responding better so that they can deal with unexpected aspects of incidents they face. The six identifiable stages are detailed below. Refer to Figure 1 which outlines the procedures for responding to computer incidents.

(1) Preparation. One of the most critical facets of responding to incidents is being prepared to respond *before* an incident occurs. Without adequate preparation, it is extremely likely that response efforts to an incident will be disorganized and that there will be considerable confusion among personnel. Preparation accordingly limits the potential for damage by ensuring response actions are known and coordinated. Actions to be taken include:

(a) Install a baseline of protection on all systems and networks. All computing components should have at least a minimum level of defense; if not, incidents can spread very quickly from system-to-system. Every local area network (LAN) server should for example have access controls set so that nobody but the LAN administrator(s) can write to system executables. Contact FIWC for recommendations concerning a suitable baseline of protection for systems.

(b) Create written incident response procedures and make them widely available. *Written* procedures work best during incidents. They should be widely distributed because there are many unexpected events during incidents, including absences of key personnel.

Widely distributing the procedures helps ensure that a critical complement of personnel with necessary knowledges will be available if and when an incident occurs.

(c) Plan communications needs. The tendency for the unexpected to occur during incidents often adversely affects ability to communicate with others. Contact lists with duty and home phone numbers in addition to primary and secondary FAX numbers of personnel to be contacted during incidents should be prepared and widely distributed. Issuing pagers to key personnel is also a wise step in preparing for incidents. Having a sufficient number of telephones approved for classified use (e.g., STU-III's) is critical in case classified incidents occur.

(d) Establish firecall procedures. Firecall procedures are procedures to provide operational continuity when there is a significant risk of prolonged failure or disruption. Assigned system administrators may not be available during a critical incident involving one or more of the systems. Ensure, therefore, that the passwords used to obtain superuser access to every system and LAN within your organization are recorded on a sheet of paper, sealed in a signed envelope, and placed in a locked container in case superuser access is needed by someone other than the assigned system administrator. Storing encryption keys for critical information in this manner is also advisable. Firecall procedures must include provisions for verifying the identity of the person who needs a password or encryption key during an emergency.

(e) Establish and employ standard backup and recovery procedures. Regularly backing up systems and data helps ensure operational continuity. This practice also enables personnel to check the integrity of systems and data---to verify whether unauthorized changes have occurred by comparing files to their corresponding backups. Because recovery is often a complex process, establishing and following recovery procedures is also a critical part of the preparation process. Standardizing these procedures makes it easier for *anyone* to perform them; during an emergency someone not assigned to a particular system or network may be called on to perform recovery procedures.

(f) Provide training to personnel. A workshop on responding to incidents can be one of the most valuable ways to help personnel at an organization learn how to handle incidents. Personnel should also be required to participate in periodic mock incidents in which written incident response procedures are followed for simulated incidents (e.g., as if a network intruder has broken into a DoN network).

(g) Obtain potentially useful tools in advance. As will shortly be explained in more detail, technical tools are often essential in successfully responding to an incident. Examples include virus detection and eradication tools, tools to restore mainframes and workstations, and incident detection tools. Order tools that you project to be critical to incident handling efforts *now* because the procurement process can be time-consuming.

(h) Inform users whom they should contact. Have stickers made that display the telephone number of your organization's INFOSEC group that can assist in case of a malicious

code incident. Ensure that a sticker is displayed visibly on every computer. Users report incidents more often and with less delay when they know whom to call.

(2) Identification. Identification involves determining whether or not an incident has occurred, and if one has, what the nature of the incident is. Identification normally begins after someone has noticed an anomaly in a system or network. Determining whether or not that anomaly is symptomatic of an incident is often difficult because apparent evidences of security incidents often turn out to indicate something less---errors in system configuration or an application program, hardware failures, and, most commonly, user errors. Typical indications of 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 necessary to obtain this access)

(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 or/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 of service or inability of one or more users to login to an account

(k) System crashes

(l) Poor system performance

(m) Unauthorized 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 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

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

Although no single one of these typical symptoms of security incidents is generally by itself conclusive, observing one or more of these symptoms should prompt you to investigate events more closely. You should in this vein work with other personnel at your organization who possess the appropriate technical and computer security knowledges to determine exactly what has occurred. Collective judgment is typically better than a single person's judgment when it comes to identifying incidents.

It is extremely important to obtain a full backup of the system in which suspicious events have been observed as soon as the possibility that a security-related incident has occurred is indicated. Perpetrators of computer crime are becoming increasingly proficient in quickly destroying evidence of their illegal activity. Unless this evidence is immediately captured by making a full backup, this evidence may be destroyed before you and others have a chance to look at it. The backup will, in addition provide a basis for comparison later in case you need to determine if any additional unauthorized activity has occurred. Be sure to safely store any backup tapes so that they will not be lost and/or stolen.

Ensure a log book is used to record the nature of suspicious events observed immediately after they've been observed. Include the name of the system, time and other details related to the observations (even though they may not seem to be very relevant at the time their recorded). Also record the names of those with whom the incident or possible incident was discussed. Careful recording of these details can assist efforts to identify the nature of an incident, develop effective solutions, and prosecute those who commit computer crime. Be sure additionally to safely store the log book.

Software packages can be helpful in identifying incidents. Virus detection packages are useful in detecting viruses. Intrusion detection tools can indicate whether someone has broken into a account on a system or has misused the system. System and network audit logs also generally provide sufficient information to facilitate deciding whether or not unauthorized activity has occurred.

As soon as someone identifies an incident, notification of cognizant authorities should occur. Section 6.e. describes detailed notification procedures.

(3) Containment. Containment, the third stage of responding to incidents, involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve using malicious code, incidents can spread rapidly, causing massive destruction and compromise of information. It is for example not uncommon to find that every workstation connected to a LAN is infected when there is a virus outbreak. The internet Worm

of 1988 successfully attacked over 6,000 computers in the U.S. in only one day. As soon as it is recognized that an incident has occurred or is occurring, immediately begin working on containing the incident.

The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. Work within your chain of command to determine whether sensitive information (and in the case of classified systems, classified information) should be left on information systems or whether it should be copied to media and taken off-line. It may similarly be best to move critical computing services to another system on another network where there is considerably less chance of interruption.

The next decision concerns the operational status of the compromised system itself. Should this system be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored? The answer depends on the type and magnitude of the incident. In the case of a simple virus incident, it is almost certainly best to quickly eradicate any viruses without shutting the infected system down. If the system is classified or sensitive, information or critical programs may be at risk, and it is generally best to shut the system down (or at least temporarily disconnect it from the network). If there is a reasonable chance that a perpetrator can be identified by letting a system continue to run as normal, risking some damage, disruption, or compromise of data may be advisable. Again, work within your chain of command to reach a decision. Continue to follow proper reporting procedures (see Section 6.e ahead) during this phase of activity by keeping others informed of the status of your efforts.

(4) Eradication. Eradicating an incident entails removing the cause of the incident. In the case of a virus incident, eradication simply requires removing the virus from all systems and media (e.g., floppy disks), usually by using virus eradication software. In the case of a network intrusion, eradication is more ambiguous. Network intrusions are best eradicated by bringing the perpetrators into legal custody and convicting them in a court of law. From a statistical viewpoint, however, the likelihood of obtaining a conviction is very small. The network intruder(s) may instead simply terminate efforts to gain unauthorized access or may temporarily terminate an attack, then attack the same system again several months later.

(5) Recovery. Recovery means restoring a system to its normal mission status. In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not in any way affect system software or data stored on the system. In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restore operation from backups. In this case it is essential to first determine the integrity of the backup itself. Once the restore has been performed, it is also essential to verify that the restore operation was successful and that the system is back to its normal condition.

(6) Follow-up. Some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in responding to incidents. Following up afterwards helps organizations

improve their incident handling procedures as well as continue to support any efforts to prosecute those who have broken the law. Follow-up activity includes the following:

(a) Analyzing what has transpired and what was done to intervene. 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?

(b) Analyzing the cost of the incident. Work within your chain of command to determine personnel time required to deal with the incident (including time necessary to restore systems). How much is the associated monetary cost? How much did the incident disrupt ongoing operations? Were any data irrecoverably lost, and, if so, what was the value of the data? Was any hardware damaged? Deriving a financial cost associated with an incident will not only help those who may be prosecuting any suspected perpetrators, but will also help your organization justify its requested budget for the upcoming fiscal year and possibly even in obtaining mid-year funding for security efforts.

(c) Preparing a report. Depending on the type of incident, a report (i.e. vulnerability, virus or hacker report as outlined in Appendices C through E) should be completed. Answers to questions in (a) and (b) above and "lessons learned" should be included in this report. This report should be disseminated widely enough that others will learn about the incident response process even if they were not involved in responding to the particular incident in question.

(d) Revising policies and procedures. Developing effective policies and procedures is an iterative process in which feedback from follow-up activity is essential. "Lessons learned" contained in the report described in (c) above should be used as the basis for modifying your activity's incident response policies and procedures.

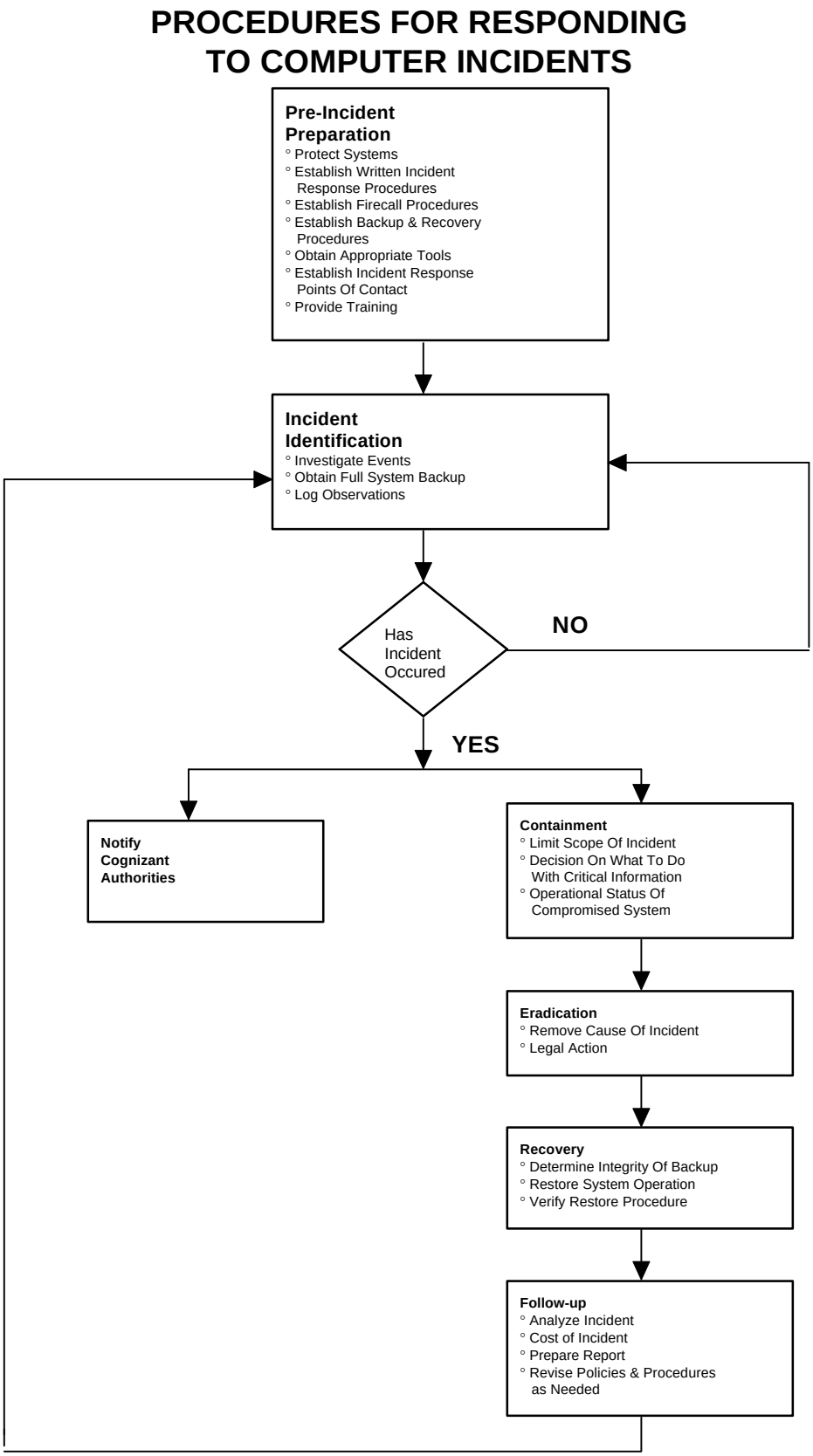

Figure 1:

c. Types of Attacks

Malicious Code Attacks

FIWC recommends that when dealing with malicious code attacks, you follow the recommended six stages of incident response. There are, however, numerous special considerations for dealing with malicious code. The following procedures will facilitate efforts to deal with malicious code incidents:

(1) Virus incidents. A virus is self-replicating code that operates and spreads by modifying executable files. Provide your users with training concerning how viruses work and the procedures that limit the spread of viruses. Viruses are user-initiated and would pose virtually no threat if every user always followed sound procedures.

Obtain the anti-virus tools needed and start using them as soon as possible. You can obtain an effective virus detection and eradication tool by contacting NISE East . A simple (but not always effective[1]) way to detect viruses is to look for unexplained increases in the length of executable files. Since viruses work by modifying applications and system executables, a growth in the length of these files typically indicates the presence of a virus. Remember, though, that saboteurs and malicious code can modify any program to which they have write access, so ensure the integrity of any anti-virus tool. A good technique is to keep at least one known good copy of anti-virus software on a write-protected floppy disk.

Immediately discontinue using any computer infected by a virus. Leave the infected computer on[2] and call technical support. Leave a quarantine sign on the computer screen to warn others to not use the computer. Do not attempt to eradicate the virus and restore the system without the assistance of a qualified technical support specialist. Make a copy of any virus that has infected a computer before it is eradicated so that your technical support team

---

Some viruses ("stealth viruses") masquerade their presence by changing the displayed length of a file to its original value even though the actual length has grown.

Studies indicate that users do far more damage to systems infected with viruses than the viruses themselves do. Leaving your computer on and calling technical support minimizes the threat of damage to your system. If the virus has "triggered," i.e., indicated its presence through some overt action such as writing a message on the screen, it will most likely have already destroyed files if it was programmed to do so. Turning your computer off at this point will, therefore, probably do no good anyway.

and/or FIWC can analyze the virus. Be sure additionally that the virus is eradicated from all backup disks. Failure to clean backup disks is the major cause of re-infections.

(2) Macro Viruses. Macro viruses are a new type of virus that use an application's own macro programming language to distribute themselves. Unlike previous viruses, macro viruses do not infect programs; they infect documents. The three macro viruses currently known by the anti-virus community are the Word Prank Macro also known as the Concept virus, the DMV virus and the Nuclear virus.

(3) Worms are 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 unusual name) is running and is consuming a large proportion of a system's processing capacity, the system may have been attacked by a worm. Worms also sometimes write unusual messages to users' displays to indicate their presence. Messages from unknown users that ask you to copy an electronic mail message to a file may also propagate worms.

Worms generally propagate themselves over networks. As such they can spread very quickly, so if a worm is noticed the system administrator or technical support specialist should be informed immediately. Saving a copy of any worm code found on a system can considerably accelerate efforts to analyze and deal with the worm. Prompt killing of any rogue processes created by the worm code minimizes the potential for damage. If the worm is a network-based worm, i.e., uses a network to spread itself, technical support should disconnect any workstations or client machines from the network unless the network is protected by very strong network defenses (e.g., firewalls). FIWC also needs to learn about any worm as soon as possible to minimize the impact of the worm across the many DoN organizations that exist.

(4) Trojan horse programs are hidden programs, often with a mi sadvertised purpose. Most malicious code is really a Trojan horse program in one way or another. A virus that disguises its presence, then executes later is technically a Trojan horse program to some degree, since the virus is hidden for part of its life cycle. Trojan horse programs are often designed to trick users into copying and executing them. Several years ago, for example, someone stood outside of the location of a technical trade fair and handed free diskettes to anyone who would take them. Although the program was supposed to determine the chances of contracting the AIDS virus, users who loaded and executed the program found that the program damaged the hard disk.

The best way to avoid Trojan horse programs is to be discriminating about using any new software that is obtained. Be especially suspicious of electronic bulletin board services, some of which may contain Trojan horse programs. If there is any doubt about the authenticity or functionality of a software program, take it to a technical support specialist who can analyze it and determine whether or not the program contains any Trojan horse code. If it is discovered that a Trojan horse program has damaged or otherwise infected a system, leave the system

alone and contact the system administrator or technical support specialist. Again, leaving a quarantine sign on the system is a wise procedure. It is generally easy to eradicate a Trojan horse program---simply delete it. Ensure that a copy of the Trojan horse program is saved (on a specially marked diskette used only for this purpose) and given to FIWC and others before the program is deleted off of the system.

(5) Cracking utilities. Cracking utilities are programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, disguising the attacker's presence, and so forth.

Cracker/Hacker Attacks

If your systems are connected to the MILNET or Internet, there is a fairly high chance that one or more cracker(s) will attack your systems sometime in the near future. Crackers (sometimes called "hackers") are unauthorized users who attempt to obtain unauthorized access to remote systems. Modem dial-in is another favorite way to crack systems. A few years ago more attacks were initiated by insiders, e.g., Navy employees or military personnel at a Navy sites, than anyone else. The nature of these attacks has, however, changed substantially over the last few years. Several years ago crackers sat at a terminal entering commands, waiting to see what would happen,then entered more commands. Today, however, most cracking attacks are automated and take only a few seconds. This makes identifying and responding to the intrusion more difficult. A recent study showed that less than one percent of system administrators whose system was penetrated by a special team both noticed the intrusions and called someone else to report the intrusions.

Protecting against a cracker/hacker attack is generally not an easy task. The best measures to adopt include always using a good (difficult-to-guess) password and setting file access permissions conservatively (e.g., so that the "world" cannot write to the home directory). System administrators should install tools such as password filters than prevent users from adopting easy-to-guess passwords and tools that check file integrity. A tool that is becoming increasingly necessary because there are so many sniffer attacks is a one-time password tool. This tool provides a list of passwords, each of which is to be used with a particular login. This prevents any password from being used successfully more than once; if a perpetrator captures a password over the network as someone remotely logs into a system, that password will not work when the perpetrator enters it.

Crackers now generally use "cracking utilities" when they obtain or attempt to obtain unauthorized remote access to systems. Cracking utilities usually are different from conventional malicious code attacks in that most cracking utilities do not disrupt systems or

destroy code[3]. Cracking utilities are typically "a means to an end"---obtaining superuser access, modifying audit logs, etc. Checksum or crypto-checksum tools are effective in spotting changes in files and are, therefore, effective in detecting cracking utilities. To use these tools you need to compute a checksum or crypto-checksum at one point in time, then compare the result to the currently obtained result. If there is a difference and if there is no readily available explanation, the integrity of the examined file may have been compromised. Remember, though, that saboteurs can modify a program to which they have access, so store the checksum/crypto-checksum programs off line and securely (e.g., on a write-locked disk stored in a safe) unless you are running them.

Indications that a system has been compromised by a hacker include most of the symptoms of incidents listed earlier in this guidebook. In particular you might notice 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, and inability to login to an account (often because someone has changed the password). In most UNIX systems[4] you can type the commands shown in Figure 2 to obtain more information about suspicious events:

Command	Displayed Information
who last	who is logged in logins/logout
acctcom	user commands entered
ps	current processes

Figure 2
Unix Commands to Access Logged Information

If these or other suspicious signs are noticed the system administrator should be notified immediately. Be sure to avoid using e-mail because many crackers can read other individual's e-mail routinely.

If a cracker is caught in the act of obtaining unauthorized access, the best course of action is to promptly determine how much danger the attack poses. If the attacker has obtained superuser access, is deleting or changing user files, or has access to a machine that supports critical Naval operations or contains sensitive data, the attack poses a

---

In conventional malicious code attacks, removing the malicious code eradicates the incident. In a cracker/hacker attack, however, removing cracking utilities does not terminate the incident. Getting the cracker to cease the unauthorized activity is the conclusive step in terminating such an incident.

In VMS the SHOW USERS command will yield information about who is using the system, and the SHOW PROCESS command will indicate which processes are running.

serious threat. In this case it is best to lock the cracker out of this system (by killing the processes the cracker has created). If on the other hand the cracker does not obtain superuser access and does not appear to be damaging or disrupting a system, it is often best to let the cracker continue to have access while authorities obtain information necessary to catch and possibly prosecute the perpetrator.

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. Leaving some or all of the cracking utilities can allow the attacker easy re-entry and possibly superuser access if the cracker attacks the compromised system again sometime later. Remember to make copies of any cracking utilities found in compromised systems and get them to FIWC. Be sure to also restore any file permissions and configuration settings that the cracker may have changed to their normal value.

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, and entries recorded in log books may conceivably be used as evidence against perpetrators.

Resolving cracker/hacker attacks is generally not easy. Not only are these attacks difficult to detect, but they also tend to be very short-lived, making them difficult to monitor and trace. FIWC is the organization which can best determine what the crackers have been doing, where the attack originated, and who the attackers are.

FIWC obtains information about incidents from the many DoN sites throughout the world and also keeps in close contact with other incident response teams. Furnishing relevant information to FIWC is, therefore, especially critical.

d. User-Detected Technical Vulnerabilities

Most of the currently known technical vulnerabilities in applications and operating systems have been discovered by users. These vulnerabilities are often discovered as users attempt to run a program or change configurations. If a technical vulnerability is discovered that can be used to subvert system or network security, immediately document that vulnerability. Record the following:

(1) What the vulnerability is

(2) How the vulnerability can defeat security mechanisms

(3) How to exploit the vulnerability (including special conditions under

which the vulnerability occurs)

After documenting the vulnerability, someone else in your organization should verify that the vulnerability exists. Then move the information up the reporting chain, as shown in the reporting chain diagram below. You should not post the vulnerability information you have discovered to the network nor should you share this information with other response teams and vendors. FIWC will coordinate with other response teams and vendors. Remember that if you find a vulnerability in a sensitive unclassified system, that vulnerability may also apply to classified systems. The vulnerability information, therefore, may be classified. Because of this possibility, following the procedures in this section may also enable you to avoid security violations.

e. Reporting Procedures

If a computer security incident is detected, it should immediately be reported to the appropriate ISSO. Each user should know how to contact the ISSO responsible for their information systems.

If the ISSO cannot be contacted, the incident should be reported to the ISSM. Again, all users need to who their ISSO is and how to contact them.

If users cannot contact either their ISSO or ISSM, they should call FIWC directly to report the incident. The timing of reporting incidents depends upon whether or not the user knows how to resolve the security incident, as shown in Figure 3.

The ISSO has the responsibility to report incident information upwards to the ISSM and FIWC in a timely fashion. Figure 4 shows a standard reporting chain. In addition, the ISSO should be prepared to advise the ISSM on immediate response decisions in the event of a serious breach of security, as in the case of an attacker gaining access via the Internet. If there is evidence of criminal activity, it is the ISSM's responsibility, in concert with the CO, to notify the Naval Criminal Investigative Service (NCIS) and co-operate with NCIS investigators. Note that if criminal activity is suspected or evident, FIWC will contact NCIS. It may be advisable for the ISSM or CO to contact NCIS directly after advising FIWC, rather than waiting for FIWC to contact NCIS.

Situation	Timing of Response
User knows how to resolve incident	Report incident to ISSO
User tries, but is unable to contact ISSO after 3 days of discovering incident	Report incident to ISSM without further delay
User tries, but is unable to contact ISSM or ISSO after 7 days of discovering incident	Report incident to FIWC without further delay
User *does not* know how to resolve incident	Promptly report incident to ISSO
User tries, but is unable to contact ISSO after 2 hours of discovering incident	Report incident to ISSM without further delay
User is unable to contact *either* ISSO *or* ISSM within six hours of discovering incident	Contact FIWC without further delay

Figure 3
Timing of Reporting Incidents

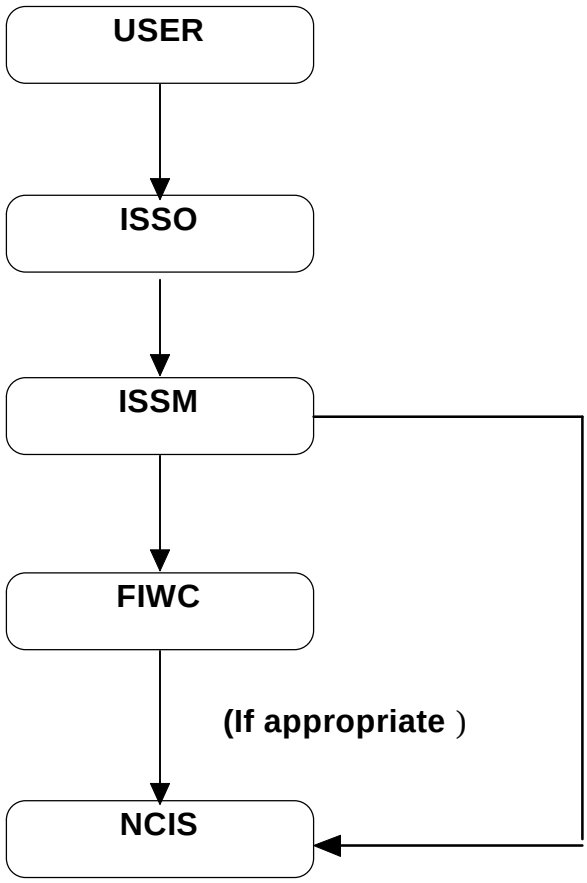

Figure 4
The Standard Reporting Chain

CAUTION: Do not disseminate information about incidents to any person, agency, or organization that is not in the reporting chain shown in the figure above. Only FIWC and NCIS have been granted the authority to share information about DoN information system security incidents with others outside this reporting chain.

f. Legal Procedures

This guidebook is not intended to provide detailed legal guidance. Legal precedent dictates, however, that you should adhere to the following procedures to avoid compromising the ability to prosecute perpetrators of computer crime.

Every DoN system should display a warning banner visible to all users who attempt to login to the system. The warning banner should advise users that the system is a U.S. Government system and only official use is allowed. Any unauthorized use may result in criminal prosecution. Remove any login banners that welcome users to a system---perpetrators may argue that they were not warned about unauthorized usage, but were instead encouraged to use a system that welcomed them. You should also include a statement in the login banner to the effect that use of a system constitutes voluntary consent to have one's computing-related activity monitored.

Another similar legal issue concerns monitoring systems and networks. Reading audit logs is *not* considered an invasion of privacy. The U.S. Department of Justice advises, however, that capturing packets that are transmitted over networks, then reading those packets verbatim constitutes a possible violation of the Electronic Privacy Act. You should not, therefore, use sniffer devices and sniffer programs to monitor the content of messages transmitted over networks, nor should you use an intrusion detection tool that does the same. Using monitoring tools that determine what *type* of packet was sent, its source and destination, etc. is not, however, problematic from a legal standpoint.

Finally, anything related in any way to an incident or possible incident is potentially a piece of evidence. As such, handling the notes you take, audit logs and backups you obtain, copies of malicious code, and so forth is critical. Soon (e.g., daily) after new information is recorded in the log book, take it to someone within your activity who is responsible for handling such evidence. This person should copy each new page of the log book, store the copy in a locked container, and provide a signed and dated receipt. Audit logs and other physical entities should be handled in the same or similar manner. If these procedures are not followed , trial attorneys for the defense may be able to successfully argue that the evidence was fabricated.

7. Conclusion.

In covering a wide range of topics related to incident response, this guidebook stresses above all else two fundamental principles. The first is the importance of following well-defined and systematic procedures for responding to security-related incidents. By enumerating six stages (preparation, detection, containment, eradication, recovery, and follow-up) of essential incident response activity, this guidebook provides a sound set of considerations to use either verbatim or as a basis for developing custom procedures tailored to specific operational environments. *The only effective way to respond to incidents is to use a structured methodology.*

Finally, even if incident response efforts are conducted systematically, they are of little value if conducted in isolation. Coordinating efforts with others is also a critical facet of incident response. Sharing data about intrusions and malicious code can for instance enable others to prevent or more quickly recognize and eradicate incidents. Cooperation among an organization's personnel can drastically reduce the manpower needed to respond to incidents, and is frequently necessary when a legal investigation is in progress. To this end FIWC plays a particularly important role within DoN. FIWC not only provides users with the information they need, but coordinates response efforts throughout DoN. Plan to more fully utilize FIWC's capabilities, therefore, as you develop and enhance your incident response strategies.

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 in those systems that have not been fixed
cracker	People who attempt to obtain unauthorized access to remote systems
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, and so forth
cryptographic	A checksum that is generated using a checksum cryptographic means. It is used to detect accidental or deliberate modification of data. See message authentication code.
encryption	Using cryptographic means to render information unintelligible in a manner that allows the information to be decrypted into its original form. The process of transforming plaintext int o ciphertext.
event	Any noticeable occurrence in a computing system
exposure	Any avenue that can lead to disruption of service or compromise and/or destruction of data
firecall	Procedures to provide operational procedures conntinuity when there is a significant risk of prolonged failure or disruption

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. [O].
FIWC	Fleet Information Warfare Center
hacker	Same as cracker
hoax	Spreading false information
incident	An adverse event (that in the context of this guidebook is related to computing systems)
Information Warfare	Tactics and methods used to affect an adversary's information infrastructure
integrity	(1) A subgoal 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 subgoal 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 (1) its meaning and completeness, (2) the consistency of its representation(s), and (3) its correspondence to what it represents. System integrity is that attribute of a system relating to the successful and correct operation of computing resources.
intrusion	Unauthorized access to a system or network
ISSO	Information Systems Security Officer
ISSM	Information Systems Security Manager
NAVCIRT	Naval Computer Incident Response Team
NCIS	Naval Criminal Investigative Service
PAO	Public Affairs Office

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.
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
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
NAVCIRT SERVICES

NAVCIRT contact information is as follows:

Phone: 1-800-628-8893
Pager: 1-800-759-7243, PIN# 5294117
Address:

Commanding Officer
Fleet Information Warfare Center
2555 Amphibious Drive
Norfolk, VA 23521-3225
ATTN: NAVCIRT

e-mail:[5] navcirt@fiwc.nosc.mil

There are currently many bulletin board and ftp services that contain valuable information not only about incident response but also computer and information security as well. The most relevant source of information to DoN users is the NISE East bulletin board. You can access this service by using ftp (file transfer protocol) to reach the following address:

infosec.nosc.mil

Other useful information is available from the following:

risks-request@csl.sri.com
cert-advisory-request@cert.org
ciac@llnl.gov
first@org
alt.security
comp.security.announce
comp.security.misc
comp.security.unix
firewalls@greatcircle.com
academic-firewalls@net.tamu.edu
research.att.com
decwrl.dec.com
coast.cs.purdue.edu

Electronic mail sent in cleartext is not very secure. Do not, therefore, use electronic mail to send sensitive information such as the names of suspects, cracking scripts discovered in compromised systems, etc. unless you use Privacy Enhanced Mail (PEM) or another encryption-based tool approved for use in U.S. Navy computing systems. Your system and the system to which you want to send the mail must both have this encryption mechanism and you must share one or more "keys" (alphanumeric strings known only to a limited set of users who need to share information) with the user with whom you want to send privacy-enhanced mail.

Information specific to viruses can be found at these sources:

http://www.first.org/virus/virus1/ (world wide web access)
computer-virus_801929995@rtfm.mit.edu

A good source of information about handling incidents are the proceedings of the Forum of Incident Response and Security Teams (FIRST) Workshops on Incident Response (available through NAVCIRT). Additional information sources include:

(1) Brock, J. Testimony before U.S. Senate Government Information Dissemination Subcommittee, November 19, 1991.

(2) Schultz, E.E. "An Analysis of Intrusions into U.S. Military Computers during Operation Desert Storm/Desert Shield." Technical report prepared for National Institute of Standards and Technology, November, 1992.

(3) Schultz, E. E. Testimony before U.S. Senate Government Information Dissemination Subcommittee, November 19, 1991.

(4) Schultz, E.E., Brown, D.S., and Longstaff, T.A.. Responding to Computer Security Incidents: Guidelines for Incident Handling . University of California Technical Report UCRL-ID-104689, 1990.

(5) Stoll, C Tracking a Spy through a Maze of Computer Espionage: The Cuckoo's Egg . New York: Doubleday, 1989.

Many tools are available to help prevent and/or respond to incidents. NAVCIRT will, for example, provide you with a copy of an anti-virus package at no cost. NAVCIRT can in addition provide you with a copy of a crypto-checksum program.

There are now many public domain tools available to help prevent and/or detect incidents. Most of these tools deal with UNIX security problems in some way. Tools include:

COPS - checks systems for security vulnerabilities, improper configurations, inappropriate modes, and easy-to-guess passwords

Courtney - detects when SATAN (see below) has been run against a system within a network

CRACK - finds easy-to-guess passwords

ICE PICK - remotely scans systems to determine whether there are vulnerabilities

NFS Watch - monitors use of the Network File System [6]

npasswd - keeps users from choosing easy-to-guess passwords

Password+- keeps users from choosing easy-to-guess passwords

PEM (Privacy Enhanced Mail) - protects the secrecy of electronic mail messages

Portwrapper - protects the portmapper (port 111) so that cracking utilities cannot steal file handles and obtain unauthorized mount access to NFS servers

SecureLib - provides a secure library of C routines

Socks - proxies gateway services securely

SWATCH - detects suspicious user activity

TCP Wrapper - protects individual host machines by accepting or denying remote service requests

Tripwire - detects changes in file integrity

Most of these tools are available through one or more of the ftp sites listed earlier in this appendix.

If you need technical assistance, the first place you should look is your own site. Your site probably has a technical support, system administration group or help desk function that can provide quick answers to your technical questions. If the assistance you need is not available at your site, your vendor representative can inform you how to reach someone who can answer your questions. Remember, too, that NISE East possesses a range of technical knowledges and abilities and is willing to assist any user within the Navy.

NFS activity is transparent to UNIX log files. Because NFS is used so much to remotely attack systems, NFS activity should be logged.

APPENDIX C

VULNERABILITY REPORT

Classification markings/Distribution statements

A. Required Information.

1. Report Date:

2. Contact:

   a. Name:

   b. Organiazation:

   c. Mailing Address:

   d. Phone Number:

   e. Position:

3. Hardware/Software:

   a. List hardware and system configuration:

   b. Software Description:

      (1) Operating system (include release number):

      (2) Describe any unique attributes - i.e., locally modified s pecial security properties:

B. Executive Summary of Vulnerability.

A description of the nature and effect of the vulnerability in as general terms as possible:

C. Description of Technical Vulnerability:

1. A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so that the

weakness or design deficiency can be repeated without further information. This scenario may include source or object code.

2. Describe the specific impact or effect of the weakness or design deficiency in terms of the following: (1) denial of service, (2) alteration of information, and/or (3) compromising of data. Cite specific examples as appropriate.

3. Indicate whether or not the affected vendor has been notified.

D. Suggested Fixes - Describe any code or procedures you may have discovered that when implemented may reduce the impact of the defined technical vulnerability.

E. Additional Information.

1. System Specifics:

   a. Location:

   b. Owner:

   c. Network connections:

   d. Security attributes:

2. System use and highest classification of data on system:

3. Additional clarifying information.

APPENDIX D

VIRUS REPORT

Provide the following information to FIWC via your ISSM.

1. Name of the infecting virus:

2. Source of the virus:

3. Other locations, within or outside of your command, possibly infected as a result of this virus:

4. Number and types of systems infected (i.e. hard disks and servers), along with the number of floppy diskettes infected:

5. Method of clean-up:

6. Number of man hours required in effort:

7. Damage or observations resulting from the virus triggering:

8. Your command name and location:

9. A point of contact at your command (i.e. ISSM) include commercial and DSN phone number:

APPENDIX E

HACKER REPORT

ORGANIZATION_____
PHONE_____

1. Report Date:

2. Incident Date:

3. Type Of Incident:

4. Individuals Involved (name/office):

5. Cost of this Incident (downtime, cost, etc.):

6. Summary of Incident and Investigation Results (e.g., number of hosts attacked, how was access obtained, how was attack identified, was a Incident Response Organization contacted prior to submission of report, etc...)

7. Supervisors Recommendations/Comments:

8. Investigating Official :

9. Local Action to Prevent Reoccurrence:

10. Recommended Action by INFOSEC Official:

11. Attack Address:

12. Physical location of system:

13. Hardware Configuration:

14. Operating System:

15. Security Software installed:

16. Highest level of data residing on system:

17. Damage or observations resulting from attack:

18. Other affected hosts/sites:

19. Your command name and location:

20. A point of contact at your command (i.e. ISSM) include commercial and DSN phone numbers)