Incident Reporting Criteria and Rationale

I. What type of activity should I report?

What type of activity you should report, and the level of detail included in your report, depends on to whom you are reporting. Your local policies and procedures may have detailed information about what types of activity should be reported, and the appropriate person to whom you should report.

A. The FedCIRC's "Incident" definition

The Federal Computer Incident Response Capability (FedCIRC) is interested in receiving reports of security incidents involving information technology resources operated by or on behalf of the Federal government. FedCIRC defines an incident as:

"An event violating an explicit or implied security policy".

This definition assumes the existence of a security policy that, while generally understood, may vary between organizations. The following types of events or activities are widely recognized as being in violation of a typical security policy. These activities include but are not necessarily limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or it's data
- unwanted disruption or denial of service
- the unauthorized use of a system for the transmission, processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

You should report any activity that you feel meets the criteria for an incident or is suspicious in nature. FedCIRC policy dictates that any information specific to organization will remain confidential unless permission from the affected agency or department is received authorizing its release.

B. The FedCIRC's incident priorities

Due to resource limitations and the growing number of incident reports, it may not be possible to immediately respond to every reported incident. Incidents must be prioritized according to their impact or severity. The following incident types receive the highest priority and are processed accordingly:

- possible life-threatening activity
- attacks on the information infrastructure, such as:
  root name servers, domain name servers, major archive sites or network access points
- widespread automated attacks
- new types of attacks or new vulnerabilities

II. Why should I report an incident?

There are several reasons to report an incident to the FedCIRC. We may be able to provide technical assistance in responding to the incident, or put you in touch with others dealing with similar activity. Incident reports allow us to collect and distribute better information about malicious activities by providing a broader baseline for analysis. Reporting incidents to the FedCIRC helps to promote greater security awareness and improve overall information assurance practices. Organizational policies or legislation may require you to report the activity to FedCIRC or another Computer Security Incident Response Team (CSIRT). Since most all of government is interconnected through the Internet, it is easy to see that vulnerabilities or risks accepted by one are ultimately shared by all. Information pertaining to security related incidents or weaknesses that is collected in isolation, fails to provide any value to government as a whole. Collaboration and correlation on such information is the foundation for establishing a strong defense strategy for the protection of the entire information infrastructure.

A. A primary part of our mission is to provide a reliable, trusted, 24-hour, single point of contact for computer security related emergencies. We facilitate communication among experts working to solve security problems and serve as the central point for identifying and correcting vulnerabilities in computer systems. When you report an incident to FedCIRC, we can provide advice and reference to technical documents, offer suggestions for containing and recovering from the event and share information about recent intruder activity. In our role as the incident response and coordination center, we may have access to information that is not yet widely available and may have considerable value to you for countering the incident.

Resource limitations and the rapidly growing number of reported incidents may prevent FedCIRC from immediately responding to reported event. Each must be prioritized according to its impact and severity.

B. We may be able to associate activity with other incidents. The FedCIRC receives reports of security incidents from various sources all over the world. In many cases, these incidents have similar characteristics or involve the same intruders. By reporting your incident, you help us collect information about recent activity in the intruder community as it relates to your incident. We may also be able to put you in touch with other sites that may be pursuing legal actions against the intruder.

C. Your report will allow us to provide better incident statistics. The FedCIRC collects statistics on the incidents reported to us. Your reports help identify vulnerabilities that are being actively exploited by perpetrators, provide information about the frequency of these attacks, and identify areas where greater community awareness is needed. These statistics are made publicly available via our web page, FedCIRC periodic reports, newsletters, bulletins and formal presentations.

D. Collaborating and sharing general information with others raises security awareness. When you report an incident to the FedCIRC, we suggest that you contact the other sites known to be involved in the activity, and that you include us in any related communications. This

benefits the other sites by alerting them to possible intruder activity on their systems. In many cases, unsuccessful probes you report may identify more serious security issues at the originating site. Additionally, contacting other sites may help you respond to your security concerns by providing more information, a different perspective, or even by identifying the intruder.

E. Your report helps us to provide you with better documents. The comments and suggestions that you provide while involved in the handling of an incident enables FedCIRC to improve on the content and delivery of alerts, advisories, and other computer security publications. Your questions help us to understand what subjects require greater attention in future documents. And taken as a whole, your reports improve our understanding of the current state of the computer security practice in government.

F. Your organization's policies may dictate incident reporting criteria. Your organization's policies may require that you report suspicious activity to the FedCIRC or your internal CSIRT. If policy calls for reporting to your local CSIRT or similar activity, observe your policy guidance. Civilian agencies and departments of the Federal government are encouraged to participate in a formal relationship with FedCIRC. The relationship is bound with a Letter of Agreement detailing procedures for reporting, sharing and protecting sensitive vulnerability and incident data. It also identifies agency or department points-of-contact to insure receipt of critical information, alerts and vulnerability notices. Reporting of incidents effecting classified systems and resources should be handled according to organizational guidelines. When in doubt, contact your local security manager for assistance. Depending on the sensitivity of the information processed on the affected system, incident related information might require special handling. In such cases, program or system specific guidance will prevail.

G. Reporting incidents is a crucial element of responsible network management. There is a strong historical precedent for communicating with other sites about security incidents. The Request for Comments document "Guidelines for the Secure Operation of the Internet" (RFC1281) states:

> "The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations. This assistance may include tracing connections, tracking violators and assisting law enforcement efforts."

III. Who should I report an incident to?

Consult your organizational security policies and procedures for specific agency guidance on incident reporting and to determine to whom such reports will be sent. If procedures do not explicitly identify to whom incident reports should

be sent, you should discuss incident reporting with your management and legal counsel before proceeding.

A. Your site security coordinator

Many security procedures identify a site security manager who serves as a central resource for handling violations of your security policies. This person may coordinate and handle all communications with FedCIRC, other incident response teams, law enforcement or other activity as appropriate.

B. Your organizational CSIRT

Many agencies and departments have an CSIRT dedicated to handling incidents involving their constituency. FedCIRC is the coordinating organization through which cross-agency incident response coordination should be facilitated. More information about FedCIRC may be found on their web page at:

http://www.fedcirc.gov

To determine if your organization is a participating FedCIRC partner or registered information recipient, you may request a roster for your respective agency by submitting an e-mail information request to ***fedcirc-info@fedcirc.gov.*** Due to the volume of information handled by the management staff, please allow 5 working days for processing.

SPECIAL NOTE: FedCIRC can only guarantee delivery of notices and bulletins if agencies and departments provide periodic updates to their contact information. Changes in e-mail address naming conventions such as:

john_q_citizen@agencyname.gov
to
john.q.citizen@agencyname.gov)

may also impede delivery if not aliased in the mail database. Inform FedCIRC when changes occur in personnel or email addresses.

C. Reports to FedCIRC

FedCIRC welcomes reports from any site experiencing a computer security problem. We encourage you to include the FedCIRC on any messages you send to other sites or CSIRTs (within the limits of your site's security policies and procedures). This information will enable us to better meet our incident coordination objectives. Contact information is available on the FedCIRC web site.

D. Other sites involved in the incident

Since perpetrators frequently use compromised hosts or accounts to attack other systems, we encourage you to report any intruder activity directly to the registered point of contact(s) of the originating host. They may be unaware of the activity involving their systems, and your note will provide the incentive to check for signs of intrusion. Please "copy" FedCIRC on any such communications.

E. Law enforcement

FedCIRC **is not** a law enforcement organization. We do not conduct criminal investigations. Our activities focus on providing technical assistance and facilitating communications in response to computer security incidents involving information technology resources under cognizance of civilian agencies and departments of the United States Government.

However, attacks or other malicious activities against Federal government systems constitute criminal action requiring mandatory law enforcement intervention. In such cases, law enforcement officials may request assistance from FedCIRC observing standard investigative procedures that ensure the preservation of Constitutional Law. If you are interested in contacting law enforcement to conduct a legal investigation, we encourage you to review your local policies and procedures for guidance. We also encourage you to discuss the intruder's activity with your management and legal counsel before contacting law enforcement. Your legal counsel can provide you with legal options and courses of action based on your organization's requirements. We do not have legal expertise and cannot offer legal advice or opinions. Agencies or departments that wish to instigate investigation actions of crimes involving the Federal computer resources may contact their organization's Office of the Inspector General, Federal Bureau of Investigation (FBI) field office or the National Infrastructure Protection Center (NIPC). To find contact information for your local FBI field office, consult your local telephone directory or see the FBI's contact web page, available at:

http://www.fbi.gov/contact.htm

Information for the NIPC may be found at:

http://www.nipc.gov

IV. What should I include in my incident report?

When reporting intruder activity, it is important to ensure that you provide enough information for the other site or CSIRT to be able to understand and respond to your report.

A. When reporting an incident to the FedCIRC, follow the guidance detailed in *attachment (1)*. The detail in your report will have a direct bearing on the accurate understanding of the intruder's activity, the resulting impact and will also contribute to development of appropriate countermeasures. Thorough reports enable FedCIRC to provide the best assistance. Detailed information reported to FedCIRC is not intended for redistribution to other organizations. Some of the supplied information may be sensitive in nature and is requested for the FedCIRC's internal use only. FedCIRC policy dictates that any information specific to your site will remain confidential unless permission to release it is received.

B. When reporting information to FedCIRC, the reporting agency should protect the information at the level appropriate with its sensitivity. PGP encrypted e-mail, secure voice (STU-III) and secure facsimile are available to receive sensitive information relative to an incident or for the exchange of sensitive information. Each reported incident will receive a uniquely assigned FedCIRC incident tracking number. Follow-up

information requests or other related information will always contain the respective reference number. These numbers aid in the tracking of correspondence and identify related activity. Ensure the appropriate reference number is included in all related correspondence. When required to correspond with another affected site, include the FedCIRC reference number for clarity. FedCIRC requests that the incident reference number be clearly displayed in the "Subject:" line of any e-mail messages regarding the incident.

Provide complete contact information when filing an incident report. Include e-mail, phone, cellular, pager, FAX and after-hours contact information as appropriate. It is also important that an alternate contact point be identified at the time of filing.

C. FedCIRC's policy for disclosing information precludes the release any information about an agencies involvement in an incident, without the explicit permission to do so. While this policy ensures that you can report intruder activity to FedCIRC in confidence, it also inhibits the process of putting you in contact with other sites involved in the incident or to share details with elements of law enforcement that may be involved in a related investigation. If permission to collaborate with other organizations is authorized, FedCIRC requests that such authorization be clearly stated in the incident report.

V. How should I report an incident to the FedCIRC?

You can report intruder activity to the FedCIRC via electronic mail, telephone hotline, or FAX machine. We encourage you to encrypt your reports to ensure your privacy, and to authenticate your identity.

A. Electronic Mail

The FedCIRC's preferred mechanism for receiving incident reports is through electronic mail. Electronic mail permits rapid prioritization for response actions and enables FedCIRC to reply to those messages quickly and efficiently. Electronic mail also provides an accurate and efficient medium for exchanging information too complex to discuss over the telephone, such as packet dumps, or large log files. Finally, electronic mail provides a reliable log of communications that we may refer to in the process of responding to an incident. The FedCIRC e-mail address for reporting incidents is: **fedcirc@fedcirc.gov**. For all other inquiries and correspondence, the e-mail address is: **fedcirc-info@fedcirc.gov**.

B. Telephone Hotline

If you have disconnected from the Internet to recover from a compromise, or if your agency is unable to send mail due to a denial of service attack, you can contact the FedCIRC on our telephone hotline. The FedCIRC incident hotline number is: **(888) 282-0870**.

Occasionally, a compromised system's electronic mail may be under surveillance by the intruder. If that is the case or if it is suspected, you are advised to use other means (telephone or FAX) to file your report.

When electronic mail is not available or provides inadequate security, and you have logs or other information that is not easily conveyed on the

telephone, you may want to send that information to us via FAX. The FedCIRC FAX machine is checked regularly. The FAX is STU-III capable (up to SECRET level) and can be reached by dialing **(412) 268-6989**.

C. Encrypting Reports to the FedCIRC

Electronic mail provides little or no privacy for the information you send across the Internet. If you wish to ensure that unauthorized persons do not read mail sent to the FedCIRC while in transit, we encourage you to use a strong encryption algorithm. The FedCIRC currently supports the use of "Pretty Good Privacy (PGP)". The FedCIRC public encryption key is available on the web site at:

http://www2.fedcirc.gov/pgp/FedCIRC_pgp-key.html.

If you encrypt messages sent to the FedCIRC, related responses will be encrypted whenever possible. Since it can be difficult for us to confirm the validity of your public PGP key, please be sure to include your public key in the body of any encrypted messages sent.

The FedCIRC signs all outgoing mail with our PGP key. If you receive any communication from us without a PGP signature, or with an invalid PGP signature, please consider the message suspect, and advise FedCIRC immediately. FedCIRC encourages all sites communicating with us to encrypt and sign their e-mail messages with PGP.

More information about PGP is available from **http://www.pgp.com**.

VI. When should I report an incident?

Incident reports that are sent shortly after the incident occurred are the most likely to be of value. This does not imply that an incident report becomes useless after some period of time. FedCIRC encourages agencies and departments to report all suspicious activity, even if the intruder's activity is quite old at the time of reporting. Other than exercising added caution to ensure that the date of the activity is clearly identified, FedCIRC encourages the reporting of the incident as you would any other incident, since other sites may not yet be aware of the incident. Remember, a report not only is the first step in recovery for your agency or department but it helps raise the awareness across government and contributes to the overall protection of the nation's critical information infrastructure.

Attachment 1 – FedCIRC Incident Reporting Criteria

When sites report incidents to us, our main goal in collecting information is to help them understand what happened, how to recover from the attack, and how to prevent it from happening again. We also collect information that will help us understand the state of Internet security and what types of attacks intruders are using so we can best inform the Internet community about how to defend their systems. Since our focus is not on legal or law enforcement issues, the information we recommend to be collected might not be the same as needed for those purposes.

When an incident reporting form is used to assist sites in handling the incident (as opposed to reporting details of an incident after the fact), we do not expect it to be able to provide all of the information necessary for us to completely assess what has happened or to provide all of the advice necessary to recover. Because reporting sites might not have all of the information available at the time of the report, or might not have the expertise
necessary to discover all of the incident details, the incident reporting form should be viewed as the first step in a dialogue to determine what has happened and the best actions to take to recover. The goal of the incident reporting form is to provide as much key information as possible at the initiation of the dialogue, so that we can provide effective recommendations to the reporting site from the start. Information needed to respond to incidents falls into several categories:

Category	**Fields**	**Need**	**Explanation**
contact information	• name • organization name • email address • phone number(s)	high	This set of information is needed to ensure that we can get in contact with the reporting site to obtain additional information or provide assistance.
demographic information	• sector type (government, energy, education, etc.)	medium	This information helps us categorize reports based on the types of organizations affected. It also can help us determine if a U.S. Government agency or an organization that is in the critical infrastructure is involved.

Category	Fields	Need	Explanation
hosts/networks involved	for attacked machines and source of attack: • host name • IP address • time zone for host • purpose of host that was attacked	medium	While host names and IP numbers are not required to provide assistance to sites, they help us collate a report with other reports to determine how widespread the activity is and to understand other technical issues relating to the attack which might have been observed at other sites, but not by the reporting site.
Attack Description	• dates of activity • methods of intrusion • intruder tools involved and any logs/output from those tools • software and operating system versions and patch levels vulnerabilities exploited • log extracts	high	This description of the activity provides us with the information we need to help the site determine what has happened and how to recover. It also allows us to give advice on steps the site can take to minimize the potential that they will be affected by this type of attack in the future.
Damage Assessment	• Cost of handling incident • Monetary damage caused by attack (lost business, etc.)	low	

Category	Fields	Need	Explanation
Permission to Contact	Does the site grant permission for us to reveal their • domain name • hosts involved • contact information • to other parties, such as • other involved sites • other response teams • law enforcement	medium	Site identifying information will not be released without explicit permission, however, such permission and release of information is rarely needed to provide advice to the reporting site on how to recover and prevent future activity
Security Tools and Methods in Use	Detailed information on the security defenses used at the site, including • authentication tools • file integrity checking tools • network monitoring tools • service filtering tools • vulnerability scanning tools • automated patch or configuration tools	low	In most cases, this information is not needed to provide advice on how to recover, however, it can be helpful in providing advice on how to prevent future attacks. Knowing what the site is using to defend their systems can help you identify areas where they can do better. Compiling this information can also help a site determine themselves where they might be deficient.