



ARMY REGULATION 15-6

INVESTIGATION GUIDE

for

INFORMAL INVESTIGATIONS

of

INTERNET PORNOGRAPHY

and

GOVERNMENT COMPUTER MISUSE

July 2003

Office of the Staff Judge Advocate
90th Regional Readiness Command

CONTENTS

Chapter 1. Introduction

| | |
|-----------------------------------|---|
| 1. Purpose | 2 |
| 2. Duties | 2 |
| 3. Authority | 2 |
| 4. Laws and Regulations | 3 |

Chapter 2. Preliminary Matters

| | |
|--|---|
| 1. Appointing Authority | 4 |
| 2. Appointment Procedures. | 4 |
| 3. Obtaining Assistance | 4 |
| 4. Suspense and Chronology | 5 |
| 5. Concurrent Investigations | 5 |

Chapter 3. Conducting the Investigation

| | |
|--|----|
| 1. Developing an Investigative Plan | 5 |
| 2. Initial Procedures in Internet Pornography Investigations | 6 |
| 3. Obtaining Evidence | 7 |
| 4. Obtaining Witness Testimony | 10 |
| 5. Article 31 and Fifth Amendment Rights Advisement | 11 |
| 6. Scheduling and Conducting Witness Interviews | 12 |
| 7. Rules of Evidence and Standard of Proof | 13 |

Chapter 4. Completing the Investigation

| | |
|---|----|
| 1. Preparing Findings and Recommendations | 14 |
| 2. Preparing the Report of Investigation for Submission to Appointing Authority | 15 |
| 3. Legal Review | 15 |

CHAPTER 1 - INTRODUCTION

1. Purpose.

a. This guide is intended to assist those officers who have been appointed as investigating officers under the provisions of Army Regulation (AR) 15-6 to conduct an informal investigation into the misuse of a government computer system.

b. This guide is based on AR 15-6, dated 30 Sep 96, and *Army Regulation 15-6 Investigation Guide for Informal Investigations*, dated Jan 97. An informal investigation is simply an administrative fact-finding procedure, normally using a single investigating officer.

2. Duties.

a. The primary duties of an investigating officer are:

- 1) to ascertain and consider the evidence on all sides of an issue,
- 2) to be thorough and impartial in conducting the investigation,
- 3) to make written findings and recommendations that are warranted by the facts and that comply with the instructions of the appointing authority.
- 4) to report the findings and recommendations to the appointing authority.

b. As the basis for this type of investigation is whether a person violated a specific U.S. Army Reserve policy, the report of investigation must also include findings on the following issues:

- 1) Is the alleged violation substantiated?
- 2) If substantiated, who committed the violation?
- 3) If substantiated, did the person knowingly and willfully commit the violation?

3. Authority.

a. AR 15-6 sets forth the procedures for conducting formal and informal investigations. This guide applies only to informal investigations involving misuse of a government computer.

b. An informal investigating officer can use whatever method he or she finds most efficient and effective for acquiring information. Informal investigation procedures are not intended to provide a hearing for persons who are the subject of the investigation. Since a respondent is not designated in an informal investigation, no one is entitled to the rights of a respondent, such as notice of the proceedings, an opportunity to participate in the proceedings, representation by counsel, or the right to call and cross-examine witnesses.

c. Only commissioned officers, warrant officers, or DA civilians in the grade of G-13 or above may be appointed as investigating officers. When choosing an informal investigating officer, the appointing authority should select the best qualified person based on their education, training, experience, length of service, and temperament. The investigating officer must also be senior to any person that is the subject of the investigation. If, during the course of the investigation, it is determined that a person senior to the investigating officer may also be a subject of the investigation, the appointing authority must be immediately notified so that another investigating officer may be appointed who is senior to the person affected.

4. Laws and Regulations.

a. AR 25-1 establishes the policies for information management and technology. Chapter 6 specifically provides that the use of DoD email and other systems, including the Internet, are limited to the conduct of official business or other authorized uses. It further provides that DoD Directive 5500.7-R, Joint Ethics Regulation (JER), Section 2-301 serves as the basis for Army policy on the use of telecommunication and computer systems. (Figure 1).

b. The U.S. Army Reserve (USAR) policy on using government resources and communication systems is stated in an Office of the Chief, Army Reserve (OCAR) memorandum, dated 28 May 1999. (Figure 2). This policy provides that Army Reserve personnel may use such resources and systems for authorized purposes only, which are specifically spelled out in the regulation. This policy is further set forth in USARC Regulation 380-2, Chapter 10, and 90th RRC Regulation 25-1, Chapter 8.

c. With the exception of child pornography, most cases involving government computer system misuse are also a violation of the Joint Ethics Regulation, but not a violation of federal law. For military personnel, a violation of the JER is considered a criminal offense under Article 92, Uniform Code of Military Justice (UCMJ).

d. However, if a certain type of misuse is not a violation of the JER, it could still be a violation of USAR or 90th RRC policy. (Figure 3). Thus the misuse could still result in adverse administrative action. This is explained in greater detail in Chapter 3.

e. As noted above, using a government computer system to receive, view, possess, reproduce and/or distribute material that contains an image of child pornography not only is a violation of the JER, it is a violation of federal law – Title 18, United States Code, Sections 2252 and 2252A. This will also be explained in greater detail in Chapter 3.

CHAPTER 2 - PRELIMINARY MATTERS

1. Appointing Authority.

- a. Under AR 15-6, Chapter 2, the following persons may appoint an informal investigation:
 - 1) Any general court-martial convening authority, including the Commander, 90th RRC.
 - 2) Any general officer, or commander at any level.
 - 3) A principal staff officer or supervisor in the grade of Major or above.
 - 4) A DA Civilian supervisor, GS-14 or above, who is the head of an agency or activity, or chief of a division or department.

2. Appointment Procedures.

a. Informal investigations may be appointed orally or in writing. A written appointment is usually in the form of a memorandum of appointment. Whether oral or written, the appointment should clearly specify the purpose and scope of the investigation and the nature of the findings and recommendations required. If the appointment orders are unclear, the investigating officer should seek clarification.

b. The primary purpose of an investigation is to report on matters the appointing authority has designated for inquiry. The appointment orders may also contain specific guidance, which, even though not required by AR 15-6, nevertheless must be followed. For example, AR 15-6 does not require that witness statements be sworn for informal investigations; however, if the appointing authority requires this, all witness statements must be sworn. A sample appointment memorandum is shown at figure 4.

3. Obtaining Assistance.

a. A Judge Advocate (JA) legal advisor will be appointed to provide assistance to the investigating officer at the beginning of, and at any time during, the investigation. Investigating officers should always seek legal advice as soon as possible after they are appointed, and as often as needed while conducting the investigation.

b. In a memorandum dated 3 Dec 99, the Commander, 90th RRC, requires that all informal investigating officers consult with their servicing JA legal advisor before beginning their investigation. (Figure 5).

c. The JA officer can assist an investigating officer in framing the issues, identifying the information required, planning the investigation, and interpreting and analyzing the information obtained. However, the JA officer is limited to only offering legal advice and assistance.

4. Suspense and Chronology.

a. Misuse of a government computer system is normally discovered externally by USARC. Occasionally, misuse is discovered internally by 90th RRC, DCS, G6 personnel.

b. If USARC discovers the misuse, they notify the Commander, 90th RRC, who then notifies the appropriate unit to take the required actions. USARC normally gives the 90th RRC a 60-day suspense to report the final results and disposition of the alleged violation. Once notified by USARC, or, if the violation is discovered internally, HQ's, 90th RRC notifies the proper unit and gives a 45-day suspense to report the results of the investigation.

c. Since time is of the essence, as soon as the investigating officer receives appointing orders, he or she should complete Section I and the first part of Section II of DA Form 1574, the Report of Proceedings.

d. Additionally, the investigating officer should begin a chronology showing the date, time, and a short description of everything done in connection with the investigation, beginning with the date the appointment orders are received. Investigating officers should also record the reason for any unusual delays in processing the case, such as the absence of witnesses or problem encountered in obtaining evidence. The chronology should be part of the final case file.

5. Concurrent Investigations. An informal investigation may be conducted before, concurrently with, or after an investigation into the same or related matters by another command or agency. In cases of concurrent investigations, investigating officers should coordinate with the other command or agency to avoid duplication of effort, and to ensure they do not interfere with criminal investigations. If available, the results of other investigations may be incorporated into the informal investigation and considered by the investigating officer. Additionally, an investigating officer should immediately coordinate with their legal advisor if he or she discovers evidence of serious criminal misconduct.

CHAPTER 3 - CONDUCTING THE INVESTIGATION

1. Developing an Investigative Plan.

a. Your primary duty as the investigating officer is to gather evidence and make findings of fact and appropriate recommendations to the appointing authority. AR 15-6, Chapter 3 contains general guidance for conducting an investigation.

b. You should develop an investigation plan that consists of:

- 1) An understanding of the facts required to reach a conclusion,
- 2) A strategy for obtaining evidence, and
- 3) A list of potential witnesses and a plan for when each witness will be interviewed.

c. You should begin your investigation by reviewing the checklist at Figure 6. This will give you a step-by-step overview of what is required to conduct a legally sufficient investigation.

d. Your next step would be to identify the information already available, and determine what additional information you will need before you can make your findings and recommendations. An important part of this is understanding the policies and regulations that govern the circumstances of the alleged misuse. Your legal advisor can assist in determining what information will be needed.

e. Once you establish what policies and regulations apply, you can determine whether the individual suspected of misconduct may have committed an offense under the UCMJ. This will help you identify any additional information you may need and decide on the order in which to interview the witnesses. It is recommended that you interview the person being investigated last. This prepares you to ask all relevant questions and minimizes the need to re-interview witnesses.

2. Initial Procedures in Internet Pornography Investigations.

a. Although the USAR policy memo, the JER, USARC Reg 380-2 and 90th RRC Reg 25-1 list specific types of unauthorized use of a government computer system, the most common type of misuse is accessing pornographic material through the Internet. USAR policy specifically prohibits using a government computer system to create, download, view, store, copy or transmit sexually oriented materials. This policy also provides that all government telecommunications equipment is subject to monitoring to ensure authorized use.

b. Each member of the 90th RRC that is an authorized user of a government computer system is on the ARNet computer network. USARC monitors the Internet traffic of each user on the ARNet through use of a proxy server, which records such Internet activity on an Internet Audit Log. (Figure 7). The USARC Information Office reviews this Internet Audit Log daily.

c. When a person reviewing an Internet Audit Log sees activity that indicates the unauthorized accessing of pornographic web sites, they notify HQ, USARC. HQ, USARC then notifies the Commander, 90th RRC, via email, of a possible violation of the USAR policy. Included in this email is a copy of the relevant Internet Audit Log pages and a notification memo directing an investigation of the incident. Once the HQ's, 90th RRC, DCS, G6 is notified of this possible violation, they inform the 90th RRC, DCS, G6 Information Assurance Officer (IAO).

d. Occasionally, the misuse is discovered internally by the 90th RRC, DCS, G6, rather than USARC. This typically occurs when a 90th RRC computer technician conducts a routine system check or maintenance on a person's government computer. Misuse includes not only accessing pornography, but engaging in the other activities prohibited by USARC policy and regulations. Examples of unauthorized use of a government computer are listed in figure 8. As soon as the technician discovers what appears to be a violation of USARC policy, he or she notifies the 90th RRC, DCS, G6 IAO, who in turn notifies the 90th RRC SJA office.

e. Once the 90th RRC DCSIM is notified of the violation, they disable the person's Internet account and send an Information Assurance Security Incident memorandum through the chain of command to the unit of the person suspected of the misconduct. That person's computer system is then disconnected from the network and sent to the 90th RRC DCSIM for safekeeping, pending the completion of the investigation.

f. It is at this point that an informal 15-6 investigation is commenced.

3. Obtaining Evidence.

a. When you receive your appointment orders, you should have the following evidence:

- 1) A copy of the USARC Internet Porn Violation notification memorandum.
- 2) A copy of the relevant pages of the USARC Internet Audit Log.
- 3) A copy of the 90th RRC Information Assurance Security Incident memorandum.
- 4) A copy of the affected person's DA Form 2A (if a military member).

b. The next step in the investigation is to determine the nature and extent of the misuse. This can only be accomplished by examining the person's confiscated government computer system stored at the 90th RRC, DCSIM section. You should contact the 90th RRC Information Assurance Officer as soon as possible in order to schedule a date and time to examine the computer at the 90th RRC.

c. If, for some reason, it is impossible to travel to the 90th RRC in order to examine the computer, contact your legal advisor and the 90th RRC Information Assurance Officer, so that alternate arrangements can be made for examining the computer.

d. In accordance with USARC policy on information systems monitoring, an investigating officer must submit a written request of what is to be reviewed on the computer as part of the investigation, along with a copy of the appointment order for the 15-6 investigation. To meet this requirement, a sample Investigating Officer Request memorandum is shown at figure 9.

e. Before you meet with the Information Assurance Officer (IAO) at the 90th RRC, you should examine the USARC Internet Audit Log and determine how many separate pornographic web sites were accessed. For purposes of your investigation, you only need to examine the information highlighted in red. If there is any indication that child pornography was accessed, this information will be highlight in red and in bold type. After examining this information, you can prepare a list of web sites to view when you go to the 90th RRC, in order to confirm misuse and determine the type and extent of pornography accessed.

f. When you meet with the 90th RRC IAO, have them access the web sites you identified from the Internet Audit Log. Once you confirmed misuse and determined the type and extent of Internet pornography accessed, you would then examine the computer itself. If the violation was not discovered by USARC, but by the 90th RRC DCSIM, you will not have an Internet Audit Log. Therefore, examining the computer will be the only method to obtain evidence of misuse. During your examination of the computer, the IAO can help you search the following areas:

- 1) Temporary Internet file folder (previously visited web sites).
- 2) History file folder (previously visited web sites).
- 3) Cookies file folder (previously visited web sites).
- 4) Personal file folder (previously visited web sites and saved material).
- 5) Favorites file folder (links to frequently visited web sites).
- 6) Recent file folder (recent files and programs accessed).
- 7) Temporary file folder (recent activity saved as temporary files).
- 8) Downloaded Program Files folder (previous programs downloaded onto computer).
- 9) Program Files folder (programs saved on the computer).
- 10) Files and folders on the Desktop.
- 11) Email Mailbox: Inbox, Sent Items & Personal folders (email traffic and attachments).

f. You are not required to search all of the above listed areas. The number of pornographic web sites recorded on the Internet Audit Log, as well as the type of pornography viewed, will be a good indicator of how extensive your search needs to be. Thus you may only need to search the Temporary Internet, History and Cookies folders, or, the misuse may be so widespread that a thorough search of all of the areas is necessary. If you have any questions about the extent of your search, consult your legal advisor and the 90th RRC DCSIM IAO.

g. However, if at any time during your examination of the computer and/or web sites, you identify material that may contain child pornography, you will immediately suspend your investigation and notify the 90th RRC SJA office. A JAG officer will then examine that material and, if it is determined to be child pornography, contact CID. If CID accepts the case, the investigation will be terminated. The 90th RRC SJA office will then notify the appointing authority that the investigation has been transferred to CID and you have no further involvement in the investigation. If CID does not accept the case, you will proceed with the investigation.

h. If, while examining the computer, you discover pornographic material, the Information Assurance Officer can make a copy that material to a CD, which will then become part of your investigation as an exhibit. The CD label should indicate it is material obtained from the computer of the person being investigated. An example would be: "15-6 Investigation of SGT Jane Doe, 468th Chemical Battalion, Examination of Computer 55.124.130.138, 10 Jun 02."

i. If the violation was discovered internally, you should also collect any sworn statements or written documents from the 90th RRC computer technicians who initially discovered the violation or were involved in the discovery of the violation. Even if the violation was discovered by USARC, 90th RRC DCSIM personnel may have been involved and may have relevant information or documents concerning the violation.

j. One area that may identify potential witnesses is the email Mailbox. If pornographic or inappropriate emails or attachments were sent to other people, they will be discovered in the Sent Items folder. If the person received pornographic email and/or attachments and opened them, they may be found in several different folders, including the Inbox and Personal Folders.

k. On the other hand, if you examine the computer but do not find any evidence of misuse or wrongdoing, that should also be documented. A recurring problem in informal investigations is lack of documentation with findings of no fault or no wrongdoing. It is just as important to support these negative findings with documentary evidence as it is to support adverse findings. Your report of investigation must include sufficient documentation to convince the appointing authority that the evidence supports the finding of no fault or no wrongdoing.

l. Once you have obtained the above evidence from the computer and 90th RRC DCSIM, and decided on which witnesses to interview, your next step is to visit the unit of the person being investigated. It is highly recommended that you call the senior full-time person at that unit in advance to schedule a time when the people you wish to interview will be there and available. When you arrive at the person's unit, you should obtain all relevant documentary evidence regarding the suspected person's duty performance before interviewing any witnesses.

m. Since your investigation will usually focus on whether the misuse or misconduct occurred while the person was in a military (AGR or Reserve) status, you need to obtain evidence of the person's duty status on the dates in question (when the misuse or misconduct occurred). The person you are investigating will be one of three types:

- 1) Full-time, Active Guard/Reserve soldier.
- 2) An Army Reservist who is also a full-time "Mil-Tech" DoD civilian employee.
- 3) An Army Reservist who has no other DoD affiliation.

n. If the soldier is AGR, you will want to obtain his or her active duty orders and unit assignment orders. If the AGR soldier was not present on any of the dates in question, you should obtain a copy of the document(s) authorizing the absence (leave form, TDY orders, etc.).

o. If the soldier is a Reservist, you should obtain their unit assignment orders, as well as the documents showing they were present and in a military status on the dates in question (AT, ADT, ADSW or RMA orders, and unit sign-in or drill attendance roster. If the Reservist is also a Mil-Tech at that unit, you should obtain their civilian work schedule record showing whether they were working in their civilian status on any of the dates in question.

p. If you are investigating a Mil-Tech Reservist, you may discover that some or all of the misuse occurred while they were in their civilian status. This information and evidence will still be included in your findings and recommendations, since their civilian supervisor may use this information in an adverse personnel action. This is covered more fully in Chapter 4.

q. The last type of documentary evidence you should collect from the unit before beginning your interviews are the forms the person suspected of misuse signed to obtain access to the USARC network, and any documents indicating expert knowledge of computer use or security.

1) Each person in the 90th RRC that uses a government computer must complete and sign a 90th RRC Form 48-R, Network Password Request Form. By signing this form the person acknowledges they have read and agree to comply with the USAR policy on using government communications systems.

2) They must also receive an information systems security briefing and sign USARC Form 75-R, Information Systems Security Briefing. Their signature indicates that they will comply with the policies and procedures governing the use of government computer services, computer networks and software.

3) You should also check to see if the person was given a special or additional duty appointment, such as Security Manager, or Information Management Officer/NCO.

4) If the unit does not have a copy of Form 48-R and Form 75-R, the 90th RRC DCSIM IAO normally keeps a copy.

r. At this point, you are finished gathering the evidence and ready to interview witnesses.

4. Obtaining witness testimony.

a. In almost all cases, witness testimony will be required. The results of the examination of the computer will influence your decision on who you wish to interview. If the misuse appears to be minimal or accidental, you may only need to interview of couple of co-workers or supervisor(s) who had knowledge of the person's duty habits and performance. If the misuse appears to be large, habitual and over a long period of time, you may want to interview several other co-workers who might have knowledge of actual misuse during duty hours.

b. The preferred interview method is in-person, although telephonic interviews may be conducted if necessary. If you conduct a telephonic interview, the information obtained during the interview should be summarized in a sworn statement for the witness's signature later. If you cannot get a sworn statement, you should document the summary of the telephone conversation in a memorandum for record. Although the direct testimony of witnesses is preferable, you may use any previous statement of a witness as evidence, sworn or unsworn, oral or written. However, the witness should be asked to confirm these previous statements for authenticity.

c. Although AR 15-6 does not require sworn statements for informal investigations, the appointing authority may require sworn statements. Under Article 136, UCMJ, military officers are authorized to administer the oath required to provide a sworn statement. (Statements taken out of the presence of the investigating officer may be sworn before an official authorized to administer oaths at the witness's location.)

d. Sworn statements are taken on DA Form 2823. Legible handwritten statements and/or a question and answer format are usually sufficient. If the witness's testimony involves technical terms that are not generally known outside their field of expertise, they should be asked to define the terms.

e. If you determine it is necessary to interview civilian witnesses, remember that you do not have the authority to subpoena witnesses, and your authority to interview civilian employees may be subject to certain limitations. Prior to interviewing civilians, you should discuss this matter with the 90th RRC Labor Counselor at (501) 771-7901. Commanders and supervisors, however, do have the authority to order military personnel and to direct Federal employees to appear before the investigating officer and testify. Civilian witnesses who are not Federal employees may agree to appear, and, if necessary, be issued invitational travel orders. This authority should only be used as a last resort if the information cannot be otherwise obtained, and only after coordinating with the legal advisor or appointing authority.

5. Article 31 and Fifth Amendment Rights Advisement.

a. All soldiers suspected of criminal misconduct must first be advised of their rights under Article 31, UCMJ. All DoD civilians suspected of criminal misconduct must be advised of their rights under the Fifth Amendment, U.S. Constitution. If, during the course of your investigation, you determine a person may have violated Section 2-301 of the JER, then they must be advised of their rights, since such a violation can be charged as criminal misconduct under the UCMJ for soldiers, and may result in punitive action for civilians. If you determine they did not violate the JER, but did violate a USARC or 90th RRC regulation, advising them of their rights is not required, but still recommended. If you have any questions about whether you should advise a person of their rights, consult your legal advisor.

b. DA Form 3881 is used to advise a person of their rights, and record that they understand their rights and elect to either waive those rights and make a statement or remain silent and request an attorney. Always provide the rights warning at the outset of the interview to those suspected of criminal misconduct.

c. If a witness elects to assert his or her rights and requests an attorney, all questioning must cease immediately. You may resume questioning only in the presence of the witness's attorney, and only if the witness consents to being interviewed. If the witness refuses to answer any questions, you must still finish your investigation to the best of your ability and make appropriate findings and recommendations based on the available evidence.

d. In some cases, you may not become aware of a witness's involvement in criminal activity until the interview has begun. If this happens, you must provide a rights warning as soon as you suspect that the witness may have been involved in criminal activity.

e. These rights apply only to information that might be used to incriminate the witness. They cannot be invoked to avoid questioning on matters that do not involve violations of criminal law. Also, only the person suspected of criminal misconduct may assert these rights.

f. If the person you are investigating agrees to provide a statement or answer your questions, you should provide that person a Privacy Act statement as well. A blank Privacy Act statement is found at figure 10.

6. Scheduling and Conducting Witness Interviews

a. As previously mentioned, the results of your examination of the Internet Audit Log and computer will help you determine which witnesses to interview and in what order. Often, information provided by one witness will raise issues to be discussed with another. Organizing your witness interviews will save time and effort that would otherwise be spent "backtracking" to re-interview prior witnesses concerning information subsequently provided. While re-interviewing may be unavoidable in some circumstances, it should be kept to a minimum.

b. Here is a suggested approach to organizing witness interviews; it is not mandatory:

1) When you are deciding on who to interview, identify the people likely to provide the best information. Start with witnesses that will provide all relevant background information and frame the issues. This will allow your interviews of key witnesses to be as complete as possible and avoid the "backtracking" described above.

2) Focus on witnesses who would have the most direct knowledge about the misuse or the suspected person's work habits. Without unnecessarily disclosing evidence obtained, try to obtain information that would support or refute information already obtained from others. In closing your interview, ask the witness if they know of any other information that may be relevant or any other persons who might have useful information.

3) It is not necessary to interview every member of the unit since few people will have information relevant to this type of investigation. Also, you do not need to interview all relevant witnesses if the facts are clearly established and undisputed.

c. Prior to conducting your interviews, you may consult law enforcement or inspector general personnel for advice on interview techniques. The following suggestions may be helpful:

1) *Prepare for the Interview.* Review the information required from that witness and prepare a list of questions or key issues to be covered. It is helpful to begin with open-ended questions like "Can you tell me what happened?" Once you develop a general outline of events, you can explore weaknesses or inconsistencies in the testimony.

2) *Ensure the Witness's Privacy.* Conduct the interview in a place free from interruptions, which will permit the witness to speak candidly without fear of being overheard. Witnesses should not be subjected to improper questions, unnecessarily harsh and insulting treatment, or unnecessary inquiry into private affairs.

3) *Focus on Relevant Information.* Unless precluded for some reason, begin the interview by telling the witness about the subject matter of the investigation. Generally, any evidence that is material and relevant to the investigation is permissible.

4) *Let the Witness Testify in Their Own Words.* Avoid coaching the witness. When their oral testimony is completed, you should assist them in preparing a written statement in their own words that presents the relevant information in clear and logical fashion.

5) *Protect the Interview Process.* It may be appropriate to direct the witness not to discuss their testimony with other witnesses or persons who have no official interest in the proceedings until the investigation is complete.

7. Rules of Evidence and Standard of Proof.

a. Because an AR 15-6 informal investigation is an administrative action, the rules of evidence normally used in judicial proceedings do not apply. Therefore, the evidence that may be used is limited by only a few rules.

1) Information must be relevant and material to the matter under investigation.

2) Information obtained in violation of a person's Article 31 or Fifth Amendment rights may still be used in administrative proceedings, unless it was obtained by unlawful coercion or inducement.

3) Privileged communications between husband and wife, priest and penitent, attorney and client may not be considered. Present or former inspector general personnel may not be required to disclose the contents of inspector general reports, investigations, inspections, action requests, or other memoranda without appropriate approval.

4) "Off-the-record" statements are not acceptable.

b. If you have any questions about the rules of evidence, consult your legal advisor.

c. Since an informal investigation is not a criminal proceeding, there is no requirement that the facts and findings be proven beyond a reasonable doubt. Unless another directive or the appointing authority establishes a different standard, your findings must be supported by "a greater weight of evidence than supports a contrary conclusion." This is the Preponderance of Evidence standard. This means that your findings should be based on evidence, which, after considering all of the evidence obtained, points to a particular conclusion that is more credible and probable than any other conclusion.

d. The weight of the evidence is not determined by the number of witnesses or volume of exhibits alone, but by considering all of the evidence and evaluating factors such as the witness's demeanor, opportunity for knowledge and ability to recall and explain events.

CHAPTER 4 - COMPLETING THE INVESTIGATION

1. Preparing Findings and Recommendations.

a. Once you have collected all of the evidence, you must review it and make your findings. You should consider the evidence thoroughly and impartially, making findings of fact and recommendations that are supported by those facts and that comply with the instructions of the appointing authority.

b. *Facts.* To the extent possible, you should fix dates, places, persons, events, and duty status definitely and accurately. You should be able to answer questions such as: What type of violation or misuse occurred? When did it occur? How did it occur? Who was involved, and to what extent? What was the duty status of the person(s) involved at the time the violation or misuse occurred?

c. *Findings.* A finding is a clear and concise statement of a fact that can be readily deduced from the evidence in the record. In developing findings, you are permitted to rely on the facts and any reasonable inferences that may be drawn from those facts. In stating your findings, you should refer to the exhibit or exhibits relied upon in making each finding. Findings (including findings of no fault or no wrongdoing) must be supported by the documented evidence contained in your report. Exhibits should be numbered in the order they are discussed in your findings.

d. *Recommendations.* Your recommendations should take the form of proposed courses of action consistent with the findings, such as corrective action, disciplinary action, and/or reactivation or removal of the soldier's network account. Your recommendations must be supported by the facts and consistent with the findings. Each recommendation should cite the specific findings that support the recommendation. You should make your recommendations according to your understanding of the rules, regulations and policies that govern the subject matter of the investigation, guided by your concept of fairness both to the Government and the individual being investigated.

2. Preparing the Report of Investigation for Submission to the Appointing Authority.

a. After you have developed your findings and recommendations, you will finish completing the DA Form 1574, Report of Proceedings by Investigating Officer. Figure 11 is a sample DA Form 1574, for both a finding of misconduct, and a finding of no misconduct. This is only meant as a general guide in how to structure your findings and recommendations.

b. Once you have completed the DA Form 1574, you should assemble the packet in the following order:

- 1) Memorandum of appointment,
- 2) Privacy Act Statement, if applicable,
- 3) Chronology, and explanation of any unusual delays, difficulties, irregularities, or other problems, if such problems were encountered in completing your investigation,
- 4) USARC Internet Porn Violation memo and Internet Audit Log, if applicable,
- 5) 90th RRC Information Assurance Security Incident memorandum,
- 6) Statements or memoranda of 90th RRC DCSIM personnel who discovered the violation and/or misuse, if applicable,
- 7) Documentary evidence, sworn statements, and applicable memoranda.

c. The final step is to submit your completed 15-6 investigation packet to the appointing authority for his or her review and approval.

3. Legal Review.

a. AR 15-6 does not require that all informal investigations receive a legal review. However, due to the nature of your investigation and the fact that your findings and recommendations may result in adverse action or will be relied on by higher headquarters, your investigation will most likely be submitted for a legal review.

b. The legal review will be requested before the appointing authority approves the findings and recommendations. After receiving the completed investigation, the appointing authority may approve, disapprove, or modify the findings and recommendations, or, he or she may return the investigation packet back to you, directing further action, such as the taking of additional evidence or making additional findings.

2-301. Use of Federal Government Resources.

a. Communication Systems. See GSA regulation 41 C.F.R. Subpart 201-21.6 (reference (h)) on use of Federal Government telephone systems. ***Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.***

(1) Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the Federal Government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

(2) Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; e-mailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:

(a) Do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization;

(b) Are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods;

(c) Serve a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of the communications system; improving the morale of DoD employees stationed for extended periods away from home; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);

(d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service); and

(e) Do not overburden the communication system, create no significant additional cost to DoD or the DoD Component, and in the case of long distance communications, charges are:

- 1 Charged to the DoD employee's home telephone number or other non-Federal Government number (third number call);
- 2 Made to a toll-free number;
- 3 Reversed to the called party if a non-Federal Government number (collect call);
- 4 Charged to a personal telephone credit card; or
- 5 Otherwise reimbursed to DoD or the DoD Component in accordance with established collection procedures;

(3) *In accordance with applicable laws and regulations, use of Federal Government communications systems may be monitored. See DoD Directives 4640.1 (reference (i)) and 4640.6 (reference (j)). DoD employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.* In addition, use of such systems is not anonymous. For example, for each use of the internet over Federal Government systems, the name and computer address of the DoD employee user is recorded by the Government and also by the locations searched.

(4) *Most Federal Government communications systems are not secure. DoD employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, secure workstations). In addition, DoD employees shall not release access information, such as passwords, to anyone unless specifically authorized to do so by the Agency Designee.* See DoD Directives 5200.28 (reference (k)) and C-5200.5 (reference (l)). DoD employees should exercise extreme care when transmitting any sensitive information, or other valued data. Information transmitted over an open network (such as through unsecure e-mail, the internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail messages may be re-sent to others by anyone in the chain.

b. Other Federal Government Resources. Other than the use of Federal Government communications systems authorized in accordance with subsection 2-301.a. of this Regulation, above; the use of Federal Government resources as logistical support to non-Federal entity events in accordance with subsection 3-211 of this Regulation, below; and the use of Federal Government time authorized in accordance with subsection 3-300 of this Regulation, below; *Federal Government resources, including personnel, equipment, and property, shall be used by DoD employees for official purposes only, except as follows:*

(1) Agency Designees may permit their DoD employees to make limited personal use of Federal Government resources other than personnel, such as typewriters, calculators, libraries, and other similar resources and facilities, if the Agency Designee determines the following:

(a) The use does not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization;

(b) The use is of reasonable duration and frequency, and made only during the DoD employee's personal time such as after duty hours or lunch periods;

(c) The use serves a legitimate public interest (such as supporting local charities or volunteer services to the community; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);

(d) The use does not put Federal Government resources to uses that would reflect adversely on DoD or the DoD Component (such as involving commercial activities; unofficial advertising, soliciting or selling; violation of statute or regulation; and other uses that are incompatible with public service); and

(e) The use creates no significant additional cost to DoD or the DoD Component.



DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF ARMY RESERVE
WASHINGTON DC 20310-2400

REPLY TO
ATTENTION OF

DAAR-ZA (25)

28 May 1999

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Reserve Policy on Use of Government Resources and Communication Systems

1. Reference. DoD Directive 5500.7-R, Joint Ethics Regulation.
2. Applicability. This policy applies to all users of the Army Reserve Network (ARNET), whether Department of the Army military and civilian employees, and contractors.
3. Purpose. This document provides U.S. Army Reserve (USAR) policy to assist employees and supervisors in defining and understanding acceptable conditions for use of Government resources and communication systems. Government resources and communication systems include, but are not limited to, personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail. This policy establishes certain privileges for employee use of Government resources and communication systems determined to be in the best interest of the Government, and the conditions under which that privilege is granted. However, this privilege does not extend to modifying such equipment, including loading personal software or making configuration changes.
4. Responsibilities. Commanders, managers, and supervisors will establish appropriate controls to ensure that government resources and communication systems are used appropriately in accordance with this policy.
5. Communications Security. Most USAR Government communications systems are not secure. USAR employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, and secure workstations). In addition, USAR employees shall not release access information, such as passwords, to anyone unless specifically authorized to do so by the Chief Information Officer or his designee. USAR employees should exercise extreme care when transmitting any sensitive information, or other valued data. Information transmitted over an open network (such as through unsecure e-mail, the Internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the Internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail message may be re-sent to others by anyone in the chain.

6. **Policy.** Employees may use Government resources and communication systems for authorized purposes only ("authorized use"). Employees will consult with their supervisors before performing any action about which they have any doubt as to whether that action falls within the definition of "authorized use" as set forth below. Commanders and supervisors with questions are encouraged to consult with Command Ethics Counselors or Chief Information Officer personnel.

a. **Authorized Use.** Authorized use is defined as activities authorized to be performed by an individual in accordance with this policy and DoD Directive 5500.7-R, Joint Ethics Regulation.

(1) **Official Use.** Official use is activity directly related to the discharge of an employee's duties in the performance of the USAR mission.

(2) **Personal Use.** As set forth below, limited personal use of Government resources and communication systems by employees during non-work time may be authorized. Use of Government resources and communication systems may be authorized for non-government purposes when such use involves minimal additional expense to the Government, is performed on the employee's non-work time, does not interfere with the USAR mission or operations, and does not violate DoD Directive 5500.7-R. This privilege to use Government resources and communication systems for non-government purposes may be revoked or limited at any time by a supervisor.

(a) Personal use is activity conducted for purposes other than official business. Authorized purposes include brief communications made by USAR employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor or home repair appointments; brief Internet searches; e-mailing directions to visiting family relatives). Personal use may also include job searching, but only when the USAR employee is job searching in response to Federal government downsizing of the employee's position.

(b) An employee's personal use of Government resources and communication systems is limited to those situations where the Government is already providing the equipment or service. An employee's use of such equipment or services will not result in any additional expense to the Government, except normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Example of acceptable personal use includes: making a few photocopies, using a computer printer to print out a few pages of material, making occasional brief personal phone calls (as defined in DoD 5500.7-R, 2-301), infrequently sending personal e-mail messages, or limited use of the Internet.

SUBJECT: U.S. Army Reserve Policy on Use of Government Resources and Communication Systems

(c) Employee non-work time is time when an employee is not otherwise expected to be addressing official business. Employees may, for example, use Government equipment during off-duty hours such as before or after a workday, lunch periods, or authorized breaks.

b. **Unauthorized Use.** Unauthorized use is not permitted. Violations will be dealt with as appropriate. Unauthorized use includes any activity that is illegal or is prohibited by this policy; disrupts or prevents authorized use; compromises privacy of other users; performs an unauthorized release of information; or impairs the integrity of information processing, storage, or transmission capability. Unauthorized use of Government equipment includes, but is not limited to:

(1) Any use that could cause congestion, delay, or disruption of service to any Government system or equipment, including the introduction of computer viruses, the sending of "letter bombs" (repeatedly mailing to an individual to deny that person access to mail service), greeting cards, video, sound, or other large file attachments, and automatic data gathering technology on the Internet and other continuous data streams (*i.e.*, RealAudio, PointCast, CNN Live), that degrade the performance of the entire network.

(2) Using Government systems as a staging ground or platform to gain unauthorized access to other systems, or circumventing or compromising the security mechanisms of the network.

(3) The creation, copying, transmission, or retransmission of chain letters or other mass mailings regardless of the subject matter.

(4) The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.

(5) Using Government equipment or service for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(6) The creation, download, viewing, storage, copying, or transmission of sexually oriented materials.

(7) Use for commercial purposes or in support of "for-profit" activities or in support of outside employment or other business activity (*e.g.*, consulting for pay, sales or administration of business transactions, sale of goods or services), including using Government equipment or services to assist relatives, friends, or other persons in such activities.

(8) Engaging in any non-Government sponsored fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity prohibited by DoD Directive 5500.7-R.

(9) Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that contradicts the agency's mission or positions or that could create the perception that the communications was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained.

(10) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information; material that is copyrighted, trade-marked, or with other intellectual property rights (beyond fair use); proprietary data; or export controlled software or data.

8. Monitoring.

a. All government owned or leased telecommunications equipment is subject to monitoring. Employee use of this equipment, authorized or unauthorized, constitutes consent to monitoring for all lawful purposes, including to ensure that their use is authorized, for management of the systems, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. During monitoring, information may be examined, recorded, copied, and used for authorized purposes.

b. Employee e-mail and Internet correspondence is the property of the USAR. Employee communications are not considered private, despite any such designation by the sender or recipient. USAR employees have no expectation of personal privacy in e-mail or Internet communications generated on Government computers and transmitted over Government servers. The existence of passwords and "message delete" functions do not restrict the USAR's ability or right to access electronic communications.

9. Sanctions for Unauthorized Use.

a. E-mail and Internet communications may be monitored or retrieved pursuant to an authorized investigation where a reasonable belief exists that communications may provide evidence of violation of the Uniform Code of Military Justice, Army regulations or policy, or DoD directive. Investigations must be authorized by the commander. Such investigations include commander's inquiries, AR 15-6 investigations, and inspector general investigations. Commanders should consult their supporting Staff Judge Advocate office before authorizing such an investigation.

DAAR-ZA (25)

28 May 1999

SUBJECT: U.S. Army Reserve Policy on Use of Government Resources and
Communication Systems

b. Unauthorized use of Government equipment or services could result in any or all of the following sanctions: loss of use or limitations on use of equipment or services, disciplinary or adverse actions, criminal penalties, and employees being held financially liable for the cost of unauthorized use.



THOMAS J. PLEWES
Major General, USA
Chief, Army Reserve

DISTRIBUTION:

Cdr, USARC
Cdr, AR-PERSCOM
Cdr, USACAPOC
Cdr, 7th ARCOM
Cdr, 9th RSC
OCAR Division Chiefs



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
1401 DESHLER STREET SW
FORT MCPHERSON, GA 30330-2000

REPLY TO
ATTENTION OF

AFRC-CII (380-19)

19 OCT 1998

MEMORANDUM FOR USARC Major Subordinate Commands
Installation Commanders
Army Reserve Intelligence Support Centers
USARC Directors/Chiefs, Coordinating, Special, and
Personal Staff Agencies and SGS

SUBJECT: Inappropriate Use of Electronic Mail (e-mail)

1. References:

- a. Title 5, Code of Federal Regulations, Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch", current edition.
- b. DOD regulation 5500.7-R, Joint Ethics Regulation, Section 2-301.
- c. Memorandum, ASD (C3I), Subject: Use of DOD Information and Telecommunications Systems, 1 Feb 97.
- d. Message, HQDA Washington DC//SAIS-ZA// DTG 151106Z Apr 98.

2. Directors, Chiefs and supervisors at all levels should make everyone using the e-mail system aware of permissible and unauthorized uses of Army e-mail. Inappropriate use of Army e-mail systems may be a basis for consideration of disciplinary action against soldiers and civilian employees.

a. E-mail users should use e-mail resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. In particular, e-mail or other telecommunications systems will not be used in a way that would

- (1) interfere with official duties,
- (2) undermine readiness,
- (3) reflect adversely on DOD or the Army (such as uses involving pornography, chain letters, unofficial advertising, soliciting or selling via e-mail,

OCT 29 1998

AFRC-CII

SUBJECT: Inappropriate Use of Electronic Mail (e-mail)

(4) and other uses that are incompatible with public service), or further any unlawful activity or personal commercial purposes.

b. Users of e-mail services will not use these services in manner that overburdens Army telecommunications systems. Users should not send e-mail that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of e-mail or e-mail systems. Such interfering uses include, but are not limited to, the use of e-mail services to:

(1) Send e-mail chain letters;

(2) "Spam", that is, exploiting listservers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail;

(3) Broadcast unnecessary advertisements of Army services;

(4) Send a "Letter-Bomb". That is, to send the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail;

(5) Broadcast e-mail messages of daily quotations, jokes, or other similar transmissions;

(6) Broadcast unsubstantiated virus warnings from sources other than system administrators; and,

(7) Direct messages to large audiences and send repeats of the same messages as "reminders".

3. In accordance with the Joint Ethics Regulation (ref 1b), all users are advised that:

a. Use of Federal Government communications systems may be monitored in accordance with applicable laws and regulations. Such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

b. Classified information will not be transmitted over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, and secure workstations).

c. Access information, such as passwords will not be released.

SUBJECT: Inappropriate Use of Electronic Mail (e-mail)

d. Extreme care should be exercised when transmitting any sensitive information, or other valued data. Information transmitted over an open network may be accessible to anyone else on the network.

4. Users should submit complaints about inappropriate electronic transmissions to the Army Reserve Program Manager, Information Systems Security (Mrs. Pat Benny, 464-8450) or send them to bennypat@usarc-emh2.army.mil. Complaints will be investigated to determine their validity. The immediate supervisor will be informed of any inappropriate use of the e-mail system, and should take appropriate disciplinary or corrective action.

5. Additional information may be obtained from Mrs. Benny, Army Reserve, Information Systems Security, at (404) 464-8450.



JAMES R. HELMLY
Brigadier General, USA
Chief Information Officer

CF:
CIO, ISSD (Mr. Leonard/Mrs. Huebener)



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY 90TH REGIONAL READINESS COMMAND
CAPTAIN MAURICE L. BRITT UNITED STATES ARMY RESERVE CENTER
8000 CAMP ROBINSON ROAD
NORTH LITTLE ROCK, ARKANSAS 72118-2205

REPLY TO
ATTENTION OF

AFRC-CAR-JA

S:
1 July 2003

MEMORANDUM FOR

SUBJECT: Appointment as Investigating Officer

1. You are hereby appointed as an investigating officer pursuant to AR 15-6 to look into the allegations that SGT Jane Doe violated the US Army Reserve Policy on the Use of Government Resources and Communication Systems on 1 April 2003 by using her government computer to access what may be pornographic web sites. Supporting documentation from the USARC CIO is enclosed. The computer workstation involved in the possible violation is AR024AC85A673 and was identified as belonging to SGT Jane Doe, 468th Chemical Battalion, North Little Rock, AR.
2. At the onset of your investigation contact the 90th RRC, Deputy Staff Judge Advocate, at 800-501-1493 x8765, for assignment of a dedicated JAG legal advisor. The legal advisor will provide you with pertinent information regarding the scope of your investigation and advise you during its pendency.
3. In your investigation, you will use the informal procedures outlined under AR 15-6. All witness statements will be sworn and recorded on DA Form 2823, if feasible. You may conduct interviews by telephone, but you will document it with a Memorandum for Record and swear to its accuracy. A guide for conducting this type of informal AR 15-6 investigation may be found at www.usar.army.mil/90thRRC/Directory/SpecialStaff/jag/PornGuide.doc.
4. If, in the course of your investigation, you suspect a soldier of committing an offense under the UCMJ, the soldier will be advised of their rights under Article 31, UCMJ, using DA form 3881, before being questioned. You may obtain assistance with these matters from your legal advisor.
5. Submit your findings and recommendations on DA Form 1574, no later than the suspense date noted above. The report of investigation must include, but is not limited to, findings on whether the violation is substantiated, and if substantiated, who committed the violation, and did the person who committed the violation knowingly and willfully commit the violation?

Encls
as

JOHN G. DOE
COL, AG, USAR
Commanding

Figure 4



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY 90TH REGIONAL SUPPORT COMMAND
CAPTAIN MAURICE L. BRITT UNITED STATES ARMY RESERVE CENTER
8000 CAMP ROBINSON ROAD
NORTH LITTLE ROCK, ARKANSAS 72118-2205

REPLY TO
ATTENTION OF

AFRC-CAR-CG (15-6)

3 December 1999

**MEMORANDUM FOR MSC COMMANDERS, STAFF & COMMAND JUDGE
ADVOCATES, AND LSO COMMANDERS**

SUBJECT: Legal Brief for AR 15-6 Investigating Officers

1. Informal investigations conducted pursuant to AR 15-6 are important tools for collecting and reporting facts for occurrences that are not part of our normal operating procedure. In some cases, the results of an AR 15-6 investigation form the basis for adverse personnel actions. These investigations, therefore, must be thorough and must be conducted in a timely manner.
2. AR 15-6, paragraph 3-0, states that before beginning an informal investigation, an investigating officer shall review all written materials provided by the appointing authority and consult with the servicing staff or command judge advocate to obtain appropriate legal advice. This legal brief should include advice on development of an investigation plan, determinations of whether witnesses need to be informed of their rights under Article 31, UCMJ, or the Fifth Amendment, U.S. Constitution, special procedures for interviewing Department of the Army civilian employees, and preparation of findings and recommendations.
3. All MSC commanders will ensure that AR 15-6 investigating officers within their commands receive such a legal briefing before beginning an investigation. This legal briefing will be sought from JA officers assigned to staff judge advocate or command judge advocate offices, not Legal Services Organizations. Investigating officers should be encouraged to consult with legal advisors during the course of investigations whenever doing so may speed the investigation or increase the effectiveness of the investigation.


DAVID R. BOCKEL
Major General, USAR
Commanding

INFORMAL 15-6 INVESTIGATION CHECKLIST

1. Preliminary Matters:

- a. Has the appointing authority appointed an appropriate investigating officer based on seniority, availability, experience, and expertise?
- b. Does the appointment memorandum clearly state the purpose and scope of the investigation, and the nature of the findings and recommendations required?
- c. Does the investigating officer have a copy of the:
 - USARC Internet Porn Violation Tasker memorandum and USARC Internet Audit Log.
 - 90th RRC Information Assurance Security Incident memorandum.
 - USAR Policy on the Use of Government Resources and Communications systems.
- d. Has the initial legal briefing been accomplished?
- e. Has the investigating officer completed Section I of the DA Form 1574 and started a chronology?

2. Conducting the Investigation.

- a. Did the investigating officer review the initial documentary evidence to gain an understanding of the facts required to reach a conclusion?
- b. Was an investigative plan developed that included a strategy for obtaining the physical evidence and a list of potential witnesses, including a plan for when each witness should be interviewed?
- c. Has the investigating officer contacted the 90th RRC Information Assurance Officer (IAO) to schedule a date and time to examine the computer?
- d. Did the investigating officer examine all areas of the computer that might reasonably contain evidence of misuse or unauthorized activity?
- e. If evidence of misuse or unauthorized activity was found, did the 90th RRC IAO copy that material to a CD, properly labeled, to be included as an exhibit in the investigation?
- f. If any evidence of possible child pornography was found, was the 90th RRC Staff Judge Advocate's Office immediately notified? If so, was the investigation terminated and turned over to CID, or did CID decline to prosecute the case and allowed the 15-6 investigation to proceed?
- g. Is the chronology being maintained in sufficient detail to identify causes for unusual delays?
- h. Did the investigating officer contact the unit of the person being investigated and schedule a date and time to interview witnesses?
- i. Was the person being investigated read his or her rights before being interviewed?
- j. Is the information collected being retained and organized as exhibits?
- k. Is routine coordination with the legal advisor being accomplished?

INFORMAL 15-6 INVESTIGATION CHECKLIST CONTINUED

4. Preparing Findings and Recommendations.

- a. Is the evidence assembled in a logical and coherent fashion?
- b. Are the findings (including findings of no fault or no wrongdoing) clearly and concisely stated and supported by the evidence?
- c. Does each finding cite the exhibit(s) that support it?
- d. Are the recommendations consistent with the findings?
- e. Does each recommendation cite the finding(s) that support it?
- f. Are the findings and recommendations responsive to the tasking in the appointment memorandum?
- g. Did the investigation address all the issues (including systemic breakdowns; failures in supervision, oversight, or leadership; program weaknesses; and other relevant areas of inquiry) raised directly or indirectly by the appointment?
- h. Was the final Report of Investigation packet correctly assembled before submission to the appointing authority?

5. Final Action.

- a. Was an appropriate legal review conducted?
- b. Did the appointing authority approve the findings and recommendations? If not, have appropriate amendments been made and approved?

| | A | B | C | D | E |
|----|---------------------------|---------|---------------|----------------|---|
| 1 | [05/31/2002:12:43:59 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.yahoo.com/ |
| 2 | [05/31/2002:12:44:00 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://us.a1.yimg.com/us.yimg.com/a1/-/flash/compac/pcc/redcompag95x30.gif |
| 3 | [05/31/2002:12:44:23 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://c2.xxxcounter.com/c0/id/2/49306/0/ |
| 4 | [05/31/2002:12:44:23 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://rt7.xxxcounter.com/c0/id/2/49306/0/ |
| 5 | [05/31/2002:12:44:23 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.wifelovers.com/ |
| 6 | [05/31/2002:12:44:23 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.wifelovers.com/graphics/samp2.jpg |
| 7 | [05/31/2002:12:44:24 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://a.123adult.com/icon.gif |
| 8 | [05/31/2002:12:44:24 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://grafix.xxxcounter.com/counter/6/0/2/49306/32406458/0000cc/0000ff/fcc00/ |
| 9 | [05/31/2002:12:44:27 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://c2.xxxcounter.com/c0/id/2/49306/0/ |
| 10 | [05/31/2002:12:44:27 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://rt7.xxxcounter.com/c0/id/2/49306/0/ |
| 11 | [05/31/2002:12:44:28 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://grafix.xxxcounter.com/counter/6/0/2/49306/32406458/9999999/ff0000/ffff00/ |
| 12 | [05/31/2002:12:44:28 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.wifelovers.com/discuss/messages/894626/894626.html |
| 13 | [05/31/2002:12:44:30 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://c2.xxxcounter.com/c0/id/2/49306/0/ |
| 14 | [05/31/2002:12:44:30 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.wifelovers.com/discuss/clicparthappy.gif |
| 15 | [05/31/2002:12:44:30 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.wifelovers.com/discuss/messages/894626/4044816.html |
| 16 | [05/31/2002:12:45:01 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/ |
| 17 | [05/31/2002:12:45:01 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/asacp.gif |
| 18 | [05/31/2002:12:45:01 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/textlabel_01.gif |
| 19 | [05/31/2002:12:45:01 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://stats.hitbox.com/buttons/fetish0.gif |
| 20 | [05/31/2002:12:45:02 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | |
| 21 | [05/31/2002:12:45:03 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://s1.hitbox.com/s?acct=FQ51120345RAFXEN0&m=wf119&n=Main+Page |
| 22 | [05/31/2002:12:45:03 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/usallag.gif |
| 23 | [05/31/2002:12:45:03 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/vgirl_01.gif |
| 24 | [05/31/2002:12:45:04 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/menultem_01.gif |
| 25 | [05/31/2002:12:45:04 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/menultem_02.gif |
| 26 | [05/31/2002:12:45:04 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/main.html |
| 27 | [05/31/2002:12:45:05 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/rape_01.gif |
| 28 | [05/31/2002:12:45:05 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/rape_03.gif |
| 29 | [05/31/2002:12:45:06 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/textlabel_03.gif |
| 30 | [05/31/2002:12:45:08 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.redway.org/grfx/textlabel_04.gif |
| 31 | [05/31/2002:12:45:08 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.tiny-virgins.com/images/index2_01.gif |
| 32 | [05/31/2002:12:45:08 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.tiny-virgins.com/images/index2_02.gif |
| 33 | [05/31/2002:12:45:08 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://www.tiny-virgins.com/images/index2_03.gif |
| 34 | [05/31/2002:12:50:25 GMT] | PROXIED | GULFCOASTdoej | 55.124.130.138 | http://212.104.197.34.8000/images/Adult/small/red2.gif |

Figure 7

USARC Internet Audit Log

For purposes of your investigation, you only need to concentrate on Five columns:

1. Column A - Date/Time group (DTG) the Internet activity occurred:
 - This is the first column on the Log.
 - Make sure you expand the column so that the entire DTG is shown, to include GMT.
 - GMT is Greenwich Mean (Zulu) Time. Since the 90th RSC is in the Central Standard Time zone, you need to calculate what time the activity occurred in Central Standard Time (CST):
 - During Daylight Savings Time (normally April – October):
 - CST is 5 hours behind GMT, so you subtract 5 hours from the DTG.
 - Thus 12:45:03 GMT is 07:45:03 CST.
 - During regular time (normally October – April):
 - CST is 6 hours behind GMT, so you subtract 6 hours from the DTG.
 - Thus 12:45:03 GMT is 06:45:03 CST.
2. Column B – How the activity was monitored by USARC filtering software:
 - This is the second column on the Log.
 - Proxied – no keywords were identified, the software didn't view it and access was allowed.
 - Viewed – keywords were identified, the software viewed it, but there were no instructions to block access to the site.
 - Denied – access was blocked to this site and the user would have seen such a message on screen.
3. Column C – ARNet user name of the person accessing the website:
 - This is normally the third column on the Log.
 - “GULFCOAST” is the name of the 90th RSC user network.
 - “doej” is the last name and first initial of the person.
4. Column D – Internet Protocol (IP) address of the computer accessing the website:
 - This is normally the fourth column. If not, uncover the next few columns until you find it.
 - This is the computer's address on the Internet.
 - This indicates the computer address the activity originated from.
5. Column E – Universal Resource Locator (URL) of the website or portion of the website accessed:
 - This is normally the eighth column. If not, uncover the columns until you find it.
 - This is the address that defines the link to a site or file on the World Wide Web.
 - A URL can be the home page of a website (i.e. www.redway.org), or
 - A URL can be embedded in a web page to provide a hypertext link to other pages (i.e. www.redway.org/grfx/vgirl_01.gif).
 - Pornographic web sites contain numerous embedded URLs on each page that will link to other pornographic web pages. Thus, even though it looks like the person accessed many different web sites, they may only have accessed one web page that had many URL links.
 - Use the Date/Time group to help determine if individual web sites were accessed. If many URLs were accessed at the same time or only several seconds apart, this indicates a single web page was accessed that contained many embedded URLs.
 - Rows 17-33 of the Log are an example of a person accessing only one web page, but which have several embedded URLs that were also recorded by the filtering software:
 - The *www.Redway.org* web page was accessed at 12:45:01.
 - This web page contained 16 URL links, which loaded on the page, and were monitored by USARC, in the next 7 seconds.
 - Note that Rows 31 –33 indicate child pornography may have been accessed.

Unauthorized Uses of a Government Computer System

Section 2-301 of the Joint Ethic Regulation provides that Federal Government communication systems and equipment, including email and Internet systems, are for official use and authorized purposes only.

The following are examples of unauthorized uses of a Government computer and/or the email system and Internet. For military personnel, a violation of the Joint Ethics Regulation can also be charged as an offense under Article 92, UCMJ – Failure to Obey a Regulation.

1. Such use adversely affects the performance of the DoD employees' official duties.
2. Such use is unreasonably long and/or unreasonably frequent, and made during the DoD employees' duty hours.
3. Job searching that is not in response to Federal Government downsizing.
4. Such use reflects adversely on DoD or the DoD Component (Army, etc.):
 - use involving pornography.
 - chain letters or mass e-mailings.
 - unofficial advertising, soliciting, or selling (except on authorized bulletin boards).
 - inappropriately handled classified information.
 - activity that is illegal (child pornography, fraud, computer hacking, etc.).

The U.S. Army Reserve Policy on Use of Government Resources and Communication Systems further restricts the conditions for authorized use of such systems and equipment. Although violating the USAR policy cannot be charged as an offense under the UCMJ, adverse action can still be taken against Department of the Army employees and contractors.

Following are examples of unauthorized uses of Government equipment:

1. Use that could cause congestion, delay, or disrupt service to any Government system:
 - introducing computer viruses or sending letter bombs.
 - sending greeting cards or video, sound, or other large file attachments.
 - using automatic data gathering technology on the Internet.
 - using continuous data streams (RealAudio, PointCast, CNN Live, etc.).
2. Using Government systems to gain unauthorized access to other systems.
3. Creating, downloading, viewing, storing, copying, or transmitting of materials related to illegal gambling, illegal weapons, terrorist activities and any other illegal activities.
4. Activities that are illegal, inappropriate, or offensive to fellow employees or the public:
 - hate speech.
 - material that ridicules on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
5. Use for commercial purposes, or in support of "for-profit" activities, or in support of outside employment or other business activity.
6. Engaging in any non-Government sponsored fund-raising activity, endorsing any product or service, participating in any lobbying activity or engaging in partisan political activity.



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY 90TH REGIONAL READINESS COMMAND
CAPTAIN MAURICE L. BRITT UNITED STATES ARMY RESERVE CENTER
8000 CAMP ROBINSON ROAD
NORTH LITTLE ROCK, ARKANSAS 72118-2205

AFRC-CAR-JA

10 July 2003

MEMORANDUM FOR DCS, G6, 90th RRC, 8000 Camp Robinson Road, North Little Rock, AR 72118

SUBJECT: Examination of SGT Jane Doe's Government Computer Pursuant to an AR 15-6 Investigation

1. The official government computer of SGT Jane Doe, 999-99-9999, 468th Chemical Battalion, Little Rock, AR, was taken from the 468th Chemical Battalion in June 2003, and sent to the 90th RSC Information Management Office, where it is currently stored, pending the outcome of the AR 15-6 investigation of SGT Jane Doe's usage of said computer. The Computer workstation is AR024AC85A673.
2. As the properly appointed Investigating Officer, and pursuant to HQ, USARC, 4 Sep 98 Policy Memorandum on Information Systems Monitoring, I request access to SGT Jane Doe's computer in order to examine her user data as well as her data files which are stored on the automated information system, which would include all internet sites visited, all downloaded program files, and all e-mails received and sent. Said access is necessary to conduct my investigation.
4. Since I cannot access SGT Jane Doe's computer without the assistance of the 90th RRC Information Assurance Officer, I will subsequently coordinate with the Information Assurance Officer the date and time I wish to examine the computers.
5. POC for this action is the undersigned at (501) 771-9999.

Encl
Memorandum of Appointment

JOHN SMITH
MAJ, AG
Investigating Officer

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. §892

PURPOSE: The purpose for soliciting your testimony is to obtain facts and to assist the Army Regulation 15-6 Investigating Officer appointed to determine whether SGT Jane Doe committed a violation of the US Army Reserve Command's Policy on the Use of Government Resources and Communication Systems.

ROUTINE USE: Your testimony will be summarized and attached to the Report of Proceedings for the above referenced investigation. The report will be forwarded to the Commander, 90th Regional Readiness Command. Any information you provide is disclosable to members of the Department of Defense who have a need for the information in the performance of their duties.

DISCLOSURE: Providing this information is voluntary. There will be no adverse effect on you for not furnishing the information other than that certain information might not otherwise be available to the commander for his or her decision on this matter.

WITNESS SIGNATURE

DATE

REPORT OF PROCEEDINGS BY INVESTIGATING OFFICER/BOARD OF OFFICERS

For use of this form, see AR 15-6; the proponent agency is OTJAG.

IF MORE SPACE IS REQUIRED IN FILLING OUT ANY PORTION OF THIS FORM, ATTACH ADDITIONAL SHEETS

SECTION I - APPOINTMENT

Appointed by Lester C. Ellis, Command Executive Officer
(Appointing authority)

on 1 June 2002 (Date) (Attach inclosure 1: Letter of appointment or summary of oral appointment data.) (See para 3-15, AR 15-6.)

SECTION II - SESSIONS

The (investigation) (board) commenced at 90th RSC, 8000 Camp Robinson Rd, North Little Rock, AR at 1400 hrs
(Place) (Time)

on 1 June 2002 (Date) (If a formal board met for more than one session, check here . Indicate in an inclosure the time each session began and ended, the place, persons present and absent, and explanation of absences, if any.) The following persons (members, respondents, counsel) were present: (After each name, indicate capacity, e.g., President, Recorder, Member, Legal Advisor.)

The following persons (members, respondents, counsel) were absent: (Include brief explanation of each absence.) (See paras 5-2 and 5-8a, AR 15-6.)

The (investigating officer) (board) finished gathering/hearing evidence at 1500 hrs on 1 July 2002
(Time) (Date)

and completed findings and recommendations at 1600 hrs on 3 July 2002
(Time) (Date)

SECTION III - CHECKLIST FOR PROCEEDINGS

| A. COMPLETE IN ALL CASES | | YES | NO ^{1/} | NA ^{2/} |
|--------------------------|--|-----|------------------|------------------|
| 1 | Inclosures (para 3-15, AR 15-6) | | | |
| | Are the following inclosed and numbered consecutively with Roman numerals: (Attached in order listed) | | | |
| | a. The letter of appointment or a summary of oral appointment data? | X | | |
| | b. Copy of notice to respondent, if any? (See item 9, below) | | | X |
| | c. Other correspondence with respondent or counsel, if any? | | | X |
| | d. All other written communications to or from the appointing authority? | | | X |
| | e. Privacy Act Statements (Certificate, if statement provided orally)? | X | | |
| | f. Explanation by the investigating officer or board of any unusual delays, difficulties, irregularities, or other problems encountered (e.g., absence of material witnesses)? | X | | |
| | g. Information as to sessions of a formal board not included on page 1 of this report? | | | X |
| | h. Any other significant papers (other than evidence) relating to administrative aspects of the investigation or board? | X | | |

FOOTNOTES: ^{1/} Explain all negative answers on an attached sheet.
^{2/} Use of the N/A column constitutes a positive representation that the circumstances described in the question did not occur in this investigation or board.

| | | YES | NO ^{1/} | NA ^{2/} |
|--|--|-----|------------------|------------------|
| 2 | Exhibits (<i>para 3-16, AR 15-6</i>) | | | |
| | a. Are all items offered (<i>whether or not received</i>) or considered as evidence individually numbered or lettered as exhibits and attached to this report? | × | | |
| | b. Is an index of all exhibits offered to or considered by investigating officer or board attached before the first exhibit? | × | | |
| | c. Has the testimony/statement of each witness been recorded verbatim or been reduced to written form and attached as an exhibit? | × | | |
| | d. Are copies, descriptions, or depictions (<i>if substituted for real or documentary evidence</i>) properly authenticated and is the location of the original evidence indicated? | × | | |
| | e. Are descriptions or diagrams included of locations visited by the investigating officer or board (<i>para 3-6b, AR 15-6</i>)? | | × | |
| | f. Is each written stipulation attached as an exhibit and is each oral stipulation either reduced to writing and made an exhibit or recorded in a verbatim record? | | | × |
| | g. If official notice of any matter was taken over the objection of a respondent or counsel, is a statement of the matter of which official notice was taken attached as an exhibit (<i>para 3-16d, AR 15-6</i>)? | | | × |
| 3 | Was a quorum present when the board voted on findings and recommendations (<i>paras 4-1 and 5-2b, AR 15-6</i>)? | | | × |
| B. COMPLETE ONLY FOR FORMAL BOARD PROCEEDINGS (<i>Chapter 5, AR 15-6</i>) | | | | |
| 4 | At the initial session, did the recorder read, or determine that all participants had read, the letter of appointment (<i>para 5-3b, AR 15-6</i>)? | | | |
| 5 | Was a quorum present at every session of the board (<i>para 5-2b, AR 15-6</i>)? | | | |
| 6 | Was each absence of any member properly excused (<i>para 5-2a, AR 15-6</i>)? | | | |
| 7 | Were members, witnesses, reporter, and interpreter sworn, if required (<i>para 3-1, AR 15-6</i>)? | | | |
| 8 | If any members who voted on findings or recommendations were not present when the board received some evidence, does the inclosure describe how they familiarized themselves with that evidence (<i>para 5-2d, AR 15-6</i>)? | | | |
| C. COMPLETE ONLY IF RESPONDENT WAS DESIGNATED (<i>Section II, Chapter 5, AR 15-6</i>) | | | | |
| 9 | Notice to respondents (<i>para 5-5, AR 15-6</i>): | | | |
| | a. Is the method and date of delivery to the respondent indicated on each letter of notification? | | | |
| | b. Was the date of delivery at least five working days prior to the first session of the board? | | | |
| | c. Does each letter of notification indicate – | | | |
| | (1) the date, hour, and place of the first session of the board concerning that respondent? | | | |
| | (2) the matter to be investigated, including specific allegations against the respondent, if any? | | | |
| | (3) the respondent's rights with regard to counsel? | | | |
| | (4) the name and address of each witness expected to be called by the recorder? | | | |
| | (5) the respondent's rights to be present, present evidence, and call witnesses? | | | |
| | d. Was the respondent provided a copy of all unclassified documents in the case file? | | | |
| | e. If there were relevant classified materials, were the respondent and his counsel given access and an opportunity to examine them? | | | |
| 10 | If any respondent was designated after the proceedings began (<i>or otherwise was absent during part of the proceedings</i>): | | | |
| | a. Was he properly notified (<i>para 5-5, AR 15-6</i>)? | | | |
| | b. Was record of proceedings and evidence received in his absence made available for examination by him and his counsel (<i>para 5-4c, AR 15-6</i>)? | | | |
| 11 | Counsel (<i>para 5-6, AR 15-6</i>): | | | |
| | a. Was each respondent represented by counsel? | | | |
| | Name and business address of counsel: | | | |
| | (<i>If counsel is a lawyer, check here <input type="checkbox"/> </i>) | | | |
| | b. Was respondent's counsel present at all open sessions of the board relating to that respondent? | | | |
| | c. If military counsel was requested but not made available, is a copy (<i>or, if oral, a summary</i>) of the request and the action taken on it included in the report (<i>para 5-6b, AR 15-6</i>)? | | | |
| 12 | If the respondent challenged the legal advisor or any voting member for lack of impartiality (<i>para 5-7, AR 15-6</i>): | | | |
| | a. Was the challenge properly denied and by the appropriate officer? | | | |
| | b. Did each member successfully challenged cease to participate in the proceedings? | | | |
| 13 | Was the respondent given an opportunity to (<i>para 5-8a, AR 15-6</i>): | | | |
| | a. Be present with his counsel at all open sessions of the board which deal with any matter which concerns that respondent? | | | |
| | b. Examine and object to the introduction of real and documentary evidence, including written statements? | | | |
| | c. Object to the testimony of witnesses and cross-examine witnesses other than his own? | | | |
| | d. Call witnesses and otherwise introduce evidence? | | | |
| | e. Testify as a witness? | | | |
| | f. Make or have his counsel make a final statement or argument (<i>para 5-9, AR 15-6</i>)? | | | |
| 14 | If requested, did the recorder assist the respondent in obtaining evidence in possession of the Government and in arranging for the presence of witnesses (<i>para 5-8b, AR 15-6</i>)? | | | |
| 15 | Are all of the respondent's requests and objections which were denied indicated in the report of proceedings or in an inclosure or exhibit to it (<i>para 5-11, AR 15-6</i>)? | | | |
| FOOTNOTES: ^{1/} Explain all negative answers on an attached sheet. ^{2/} Use of the N/A column constitutes a positive representation that the circumstances described in the question did not occur in this investigation or board. | | | | |

SECTION IV - FINDINGS (para 3-10, AR 15-6)

The (investigating officer) (board), having carefully considered the evidence, finds:

If A Violation Was Substantiated:

The allegation of a violation of the US Army Reserve policy on the use of a government computer system is substantiated.

SGT Jane Doe, 468th Chemical Battalion, North Little Rock, AR, knowingly and wilfully accessed pornographic web sites on 31 May 2002. By her own admission (Exhibit E), SGT Doe accessed pornographic web sites during duty hours. SGT Doe stated that she was relying on the system filters to determine whether or not she should be able to view a particular web site. SGT Doe saved or stored numerous images of pornographic material on her computer (Exhibit K) and saved several links to pornographic web sites in her "Favorites" folder (Exhibit J). The e-mail system was searched but there was no evidence that she sent or received any of the pornographic material being viewed. There is also no evidence that SGT Doe accessed or attempted to access child pornography. The web site links on the USARC Internet Audit Log (Exhibit B) that appeared to be child pornography, were embedded links in the web site home page SGT Doe accessed, but did not actually link to the child pornography site.

According to SGT Doe's 1SG and company commander, she has a good work history, displays a good attitude, and never misses work (Exhibits L and M).

If A Violation Was Not Substantiated:

Explain what evidence you gathered that shows SGT Doe did not access those web sites indicated on the Internet Audit Log. This could occur if someone hacked into SGT Doe's computer system, or someone stole SGT Doe's User ID and Password and used the computer system without SGT Doe's knowledge, or SGT Doe left her computer unsecured and was away from the computer for a period of time and someone used the computer while she was away. In the last case, SGT Doe would still have violated the policy on physical security of communications equipment.

SECTION V - RECOMMENDATIONS (para 3-11, AR 15-6)

In view of the above findings, the (investigating officer) (board) recommends:

Your recommendations need to be consistent with the findings.

You should make a recommendation on the type of action to be taken by the chain of command for the misconduct/violation. This would be based on:

- whether it was a one-time occurrence or habitual, long-term viewing of pornography;
- the amount of pornographic or inappropriate material saved or stored on the computer;
- whether the pornographic or inappropriate material was emailed to others;
- whether the violation is a violation of the JER, and thus a violation of the UCMJ, or whether it was a violation of a local regulation;
- whether there is a likelihood the misconduct will continue if serious action is not taken.

You should also make a recommendation on whether the person should have their ARNet account privileges restored and if any restrictions should be placed on their computer activity, and that the computer system be returned to the unit.

SECTION VI - AUTHENTICATION (para 3-17, AR 15-6)

THIS REPORT OF PROCEEDINGS IS COMPLETE AND ACCURATE. (If any voting member or the recorder fails to sign here or in Section VII below, indicate the reason in the space where his signature should appear.)

(Recorder)

(Member)

(Member)

Your Signature

(Investigating Officer) (President)

(Member)

(Member)

SECTION VII - MINORITY REPORT (para 3-13, AR 15-6)

To the extent indicated in Inclosure _____, the undersigned do(es) not concur in the findings and recommendations of the board. (In the inclosure, identify by number each finding and/or recommendation in which the dissenting member(s) do(es) not concur. State the reasons for disagreement. Additional/substitute findings and/or recommendations may be included in the inclosure.)

(Member)

(Member)

SECTION VIII - ACTION BY APPOINTING AUTHORITY (para 2-3, AR 15-6)

The findings and recommendations of the (investigating officer) (board) are (approved) (disapproved) (approved with following exceptions/substitutions). (If the appointing authority returns the proceedings to the investigating officer or board for further proceedings or corrective action, attach that correspondence (or a summary, if oral) as a numbered inclosure.)

INDEX

Enclosures

- Encl 1 Memorandum of Appointment
- Encl 2 Privacy Act Statement
- Encl 3 Chronology
- Encl 4 Explanation of Difficulties

Exhibits

- Exhibit A USARC Internet Porn Violation Tasker #999 Memo, dated 1 Jun 03
- Exhibit B USARC Internet Audit Log for 55.124.130.138
- Exhibit C 90th RRC Information Assurance Incident memo, dated 1 Jun 03
- Exhibit D Rights Warning Certificate for SGT Jane Doe
- Exhibit E Sworn statement of SGT Jane Doe
- Exhibit F SGT Jane Doe's 90th RRC Form 48-R
- Exhibit G SGT Jane Doe's USARC Form 75-R
- Exhibit H Investigating officer's request to examine SGT Jane Doe's computer
- Exhibit I SGT Jane Doe's *Temporary Internet Files* folder
- Exhibit J SGT Jane Doe's *Favorites* folder
- Exhibit K Stored images on SGT Jane Doe's computer
- Exhibit L Sworn statement of 1SG Hulka
- Exhibit M Sworn statement of CPT Patton
- Exhibit N SGT Jane Doe's DA Form 2A, dated 15 Jun 02

CHRONOLOGY

- 1 Jun 03 Received AR 15-6 appointment orders with case file.
- 1 Jun 03 Reviewed case file and received legal briefing from 90th RRC SJA.
- 3 Jun 03 Confirmed with CPT Smith, 90th RRC Information Assurance Officer, on the location of SGT Doe's confiscated computer and suspended LAN access.
- 9 Jun 03 Received requested memoranda and policies from CPT Smith, 90th RRC Information Assurance Officer.
- 9 Jun 03 Examined SGT Doe's computer with the assistance of CPT Smith.
- 10-12 Jun 03 Reviewed evidence obtained during examination of SGT Doe's computer.
- 15 Jun 03 Coordinated with SGT Doe's full-time supervisor, Mr. Brown, to schedule my interview date and time.
- 1 Jul 03 Visited SGT Doe at her unit, 468th Chemical Battalion, North Little Rock. Also spoke with SGT Doe's 1SG and company commander.
- 2-3 Jul 03 Drafted findings and recommendations.
- 3 Jul 03 Completed AR 15-6 informal investigation and submitted report to 90th RRC SJA for legal review.