

Criminal

Investigative

Policy &

Oversight



Evaluation of Defense Criminal Investigative Organization
Programs for Investigating Computer Crimes

Report Number 9850002R

September 1, 1998

Office of the Inspector General
Department of Defense

Additional Information and Copies

To obtain additional copies of this evaluation report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Evaluations

To suggest ideas for or to request future evaluations, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Evaluation Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ACIRS	Automated Criminal Information Reporting System
AFOSI	Air Force Office of Special Investigations
ASIM	Automated System Information Monitor
CCI	Computer Crime Investigation (Air Force)
CCIT	Computer Crimes Investigation Team (Army)
CIO	Computer Investigations and Operations Department (Navy)
DCIS	Defense Criminal Investigative Service
DCIOs	Defense Criminal Investigative Organizations
FIWC	Fleet Information Warfare Center
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
LAN	Local Area Network
LIWA	Land Information Warfare Activity
MCIOs	Military Criminal Investigative Organizations
NCIS	Naval Criminal Investigative Service
SCERS	Seized Computer Evidence Recovery Specialist
USACIDC	U.S. Army Criminal Investigation Command



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

September 1, 1998

MEMORANDUM FOR COMMANDER, UNITED STATES ARMY CRIMINAL
INVESTIGATION COMMAND
DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE
SERVICE
COMMANDER, AIR FORCE OFFICE OF SPECIAL
INVESTIGATIONS
DIRECTOR, DEFENSE CRIMINAL INVESTIGATIVE
SERVICE

SUBJECT: Evaluation Report on Defense Criminal Investigative Organization Programs
for Investigating Computer Crimes (Report No. 9850002R)

We are providing this final report for review and comment. We considered management comments on a draft of this report in preparing the final report.

We appreciate the courtesies extended to the evaluation staff. Questions on the evaluation should be directed to Mr. Bruce Drucker, at (703) 604-8773 (DSN 664-8773) (BDrucker@dodig.osd.mil) or Ms. Carol Ann Brown, at (703) 604-8712 (DSN 664-8712) (CBrown@dodig.osd.mil). If management requests, we will provide a formal briefing on the evaluation results. See Appendix C for the report distribution.

A handwritten signature in black ink, appearing to read "Charles W. Beardall", is positioned above the typed name.

Charles W. Beardall
Deputy Assistant Inspector General
Criminal Investigative Policy and Oversight

Office of the Inspector General, DoD

Report No. 9850002R
(Project No. 7OG-9022)

September 1, 1998

Defense Criminal Investigative Organization Programs to Investigate Computer Crimes

Executive Summary

Introduction. We performed this evaluation to determine the current status of the Defense Criminal Investigative Organizations programs to investigate computer crimes.

Evaluation Objectives. The evaluation objectives were to:

- o document the programs the Defense Criminal Investigative Organizations (DCIOs) have in place to investigate computer crimes and computer intrusions; and
- o identify the resources devoted to the programs.

Evaluation Process. We interviewed DCIO officials at the headquarters offices of DCIOs, reviewed DCIO case summaries, and compiled from DCIO databases statistics that involved computer crimes and computer intrusions.

Evaluation Results.

o The Air Force Office of Special Investigations (AFOSI) established a computer crime investigation program in the 1970s, the Naval Criminal Investigative Service (NCIS) in 1994, and the Army Criminal Investigation Command (USACIDC) and the Defense Criminal Investigative Service (DCIS) in 1998. Only the Air Force presently has real-time capability to detect intrusion in its Service's computer systems. The Air Force computer crimes laboratory is being converted to the Department of Defense computer crimes laboratory, with funding and personnel to be provided by all military Services and DCIS. While the DCIOs have generated investigative results for a number of years in cases that involve theft, damage, and destruction of computer hardware and software, computer intrusion investigations have been less frequently conducted to date, and statistical data is more limited.

o By the end of fiscal year 1998 (FY1998), the DCIOs will average 30 full-time personnel assigned to computer crimes investigations. In addition, all DCIOs have field agents who have received advanced computer training, but who are not assigned full-time to conduct computer crimes investigations. For FY1998, AFOSI and NCIS budgeted or requested over \$3 million each in support of their programs. Start-up costs for USACIDC were estimated at \$442,000. Training for agents is consistent among the DCIOs and relies heavily on the Federal Law Enforcement Training Center (FLETC) or

DCIOs and relies heavily on the Federal Law Enforcement Training Center (FLETC) or FLETC-equivalent courses for agents, supplemented by other training available from other law enforcement and private industry training sources.

o Competition with the private market makes recruiting and retention of qualified, experienced agents to conduct computer crimes investigations a concern to all the DCIOs. Lack of timely notification of intrusions, inability of the DCIOs to maintain real-time monitoring of Departmental systems, constant training to keep up with technology and hacker activities, funding, and management support within the Department were additional concerns expressed by DCIO management as issues that affect their ability to conduct effective computer intrusion investigations.

Management Comments. Comments received from the Army and Navy are included as Appendix D. All suggestions from the Army were incorporated, and most from the Navy were as well. NCIS provided changes to statistics to Tables 1 and 2 that are different because of the differences in definitions of computer crimes. The statistics reflected in Tables 1 and 2 were derived from the Inspector General's Semiannual Reports to Congress, and were retained to maintain conformance with those previously issued documents.

Table of Contents

Executive Summary	i
Part I – Evaluation Results	
Evaluation Background	2
Description of Computer Investigation Programs	3
Resourcing of Computer Investigation Programs	10
Program Concerns	15
Part II – Additional Information	
Appendix A. Individuals Visited or Contacted	20
Appendix B. Prior Evaluations	21
Appendix C. Report Distribution	23
Part III - Management Comments	
Department of the Army Comments	26
Department of the Navy Comments	28

Part I - Evaluation Results

Evaluation Background

Evaluation Objectives. The objectives for the evaluation were to:

- o document the programs the DCIOs have in place to investigate computer crimes and computer intrusions; and
- o identify the resources devoted to the programs.

Evaluation Process. To assess the computer crimes programs, we interviewed DCIO officials at headquarters offices, reviewed case summaries, and summarized statistics provided by each DCIO and those derived from historical files for the Inspector General's Semiannual Report to Congress.

Special Considerations. We have not reviewed recent legislation or the impact it might have on investigations, nor have we attempted to discuss unresolved legal issues, such as how the Posse Comitatus Act can affect an MCIO intrusion investigation or how to authorize or conduct a search and seizure in cyberspace.

Documents and Computer-Process Data Reviewed. AFOSI Manual 71-103, Volume 5; USACIDC Manual 195-1, Chapter 12; Vice Chief of Staff, Army, directed message; current investigative case summaries; and data underlying the Inspector General's Semiannual Reports to Congress from 1994 through 1997.

Contacts During the Evaluation. We visited each Headquarters where we conducted interviews and obtained details on agent strength levels, budget, and caseloads. Further details are available upon request.

Evaluation Period, Standards, and Prior Coverage. This program evaluation was performed from January through March 1998, in accordance with standards implemented by the Inspector General, DoD. While the General Accounting Office, Army Audit Agency, and Inspector General, DoD, have published reviews on the general topic of computer systems security (Appendix B), we identified no published reviews on criminal investigations involving computers or computer intrusions.

Description of Computer Investigation Programs

Mission, scope of investigative activity, and interface among Military Service and DoD programs are presented in this section. AFOSI established a computer crime investigation program in the 1970s, NCIS in 1994, and USACIDC and DCIS in 1998. Only the Air Force presently has real-time capability to detect intrusion in its Service's computer systems. The Air Force computer crimes laboratory is being converted to the Department of Defense computer crimes laboratory, with funding and personnel to be provided by all military Services and DCIS. The Army also has computer forensic expertise as part of its general crimes laboratory at Ft. Gillem, GA. While all DCIOs have generated investigative results for a number of years in cases that involve theft, damage, and destruction of computer hardware and software, they have not conducted many investigations of computer intrusions, and statistical data from intrusion cases is more limited.

Army. USACIDC recognized a need to develop specialized investigative talent to address the Army's comprehensive move toward digitization of all its operations and support functions. The Army of the 21st Century will rely heavily on automation for networking of computers in peacetime and war, for its classified systems, for its systems connected to the internet, for its management of supplies and personnel, and for the need to protect the Army's information systems infrastructure so that logistics systems can deliver people and supplies when and where needed. The Army sees these needs as vital to its future warfighting ability.

In response to these needs, USACIDC created its Computer Crimes Investigation Team (CCIT) in January 1998. The team has as its primary responsibility investigation of computer intrusions and other complex or sensitive computer crimes that have an Army interest. Secondary responsibilities include the provision of technical assistance to field units and liaison with the Land Information Warfare Activity (LIWA), U.S. Army Intelligence and Security Command. The team is also responsible for monitoring computer-related crime trends, serving as the focal point for USACIDC operational needs, creating and updating training requirements, recommending and reviewing policy, and updating and disseminating policy to field elements.

USACIDC's field investigative units are organized in 12 districts worldwide. At the district level, advanced computer crimes agents (district coordinators) will be the district focal point for notification by LIWA of intrusions. They also will provide assistance in the proper seizure of computer evidence for crimes identified in their district, provide assistance in preparation of computer-related search warrants, assist in creating computer crimes training programs, respond to field needs in advance of arrival of the CCIT team, act as the district point of contact with the headquarters CCIT team, review crime prevention surveys, ensure crime prevention surveys are accomplished, prepare criminal intelligence

Description of Computer Investigation Programs

reports, provide computer crime awareness briefings, develop sources, conduct target analyses, and supervise and monitor the activities of subordinate offices.

The CCIT goals include receiving simultaneous, real time notification of intrusions that Information Systems Managers at attacked installations report to the LIWA, providing investigative support, being the focal point for computer investigations, providing technical expertise to the field and technical experts for testimony in trials, conducting routine data recovery from computer media, and publishing an agent's guide to computer investigations.

USACIDC does not presently have either the staff or hardware to detect intrusions real-time. Instead, they rely on notifications made by local commanders relayed through the LIWA. However, USACIDC officials commented that local commanders sometimes do not realize the importance of making a notification to the LIWA, particularly when an intrusion attempt is unsuccessful. Thus, the Army is not able to assess accurately the extent of the threat to Army systems. On February 18, 1998, the Army Vice Chief of Staff ordered the Army Signal Command to unify the Army's network and systems management and information systems security functions. The goals are to establish a near-real-time ability to detect and react to intrusions and to protect the Army's computerized information environment. Funding is to be provided at the Army level. When implemented, the centralized system should enhance USACIDC's ability to react to computer intrusions and intrusion attempts more effectively.

USACIDC's Automated Criminal Information Reporting System (ACIRS) tracks cases and preliminary information by type of computer crime. Primary case categories include computer intrusions, transmission of pornography (child pornography being an identifiable subcategory), concealing evidence of a crime on a computer, destruction and theft of data, sabotage, terrorism, warfare, technology transfer, data manipulation, trafficking in passwords or access codes, obtaining classified information, financial or credit information, and unsuccessful attempts to accomplish any of the preceding. While ACIRS tracks specialized offense codes, USACIDC officials acknowledge that quantification of case types depends upon what secondary and tertiary codes the field agent initiating the case inputs to the system.

Navy. Prior to 1995, the Navy had no requirement for centralized reporting of intrusions into Navy or Marine Corps computer networks. In 1995, the Navy began requiring all Navy commands to report all computer intrusions to the Fleet Information Warfare Center (FIWC), Little Creek, VA. In 1996, NCIS and FIWC established a formal relationship through a Memorandum of Understanding. Following implementation of the Memorandum of Understanding, intrusions reported have increased from 7 in 1994 to 148 in 1997. NCIS attributes the increase in reporting to wider connectivity within the Navy, better command-level reporting procedures, better response by NCIS to Navy commands, and better administrative support by the Navy and Marine Corps to victims.

NCIS views "computer crime" as those cases which include computers being used as the means or tool to commit an offense; a repository for data or other evidence of an offense; or as the target of an act that affects the confidentiality, integrity, or availability of sensitive data or network communications. Investigative considerations by NCIS include the theft, damage, or destruction/corruption of

hardware or software where the computer is the sole target of the offender. For example, a command may report the theft of a laptop computer as a relatively minor monetary loss, but to NCIS the value of the information stored on the computer may be significantly higher from a classification, proprietary, economic, or access perspective.

NCIS established its Computer Crime Investigations Support Unit in December 1994 with part-time field investigators and system administrators who provided "as needed" technical support to the agents. In 1996, NCIS assigned agents to the FIWC to monitor computer intrusions and virus attacks on Navy computers. These agents assist in coordinating the receipt of intrusion reports with NCIS field elements responsible for conducting the intrusion investigations.

The Computer Crime Investigations Support Unit was reorganized in 1997 into the Computer Investigations and Operations Department (CIO), which is organized into three divisions: Investigations and Operations, Integration, and Training. The Investigations and Operations Division's primary responsibility is to investigate intrusions against Department of Navy computer systems and to provide media analysis¹ support to field investigators when a computer is used in the commission of an offense, such as pornography. The Integration Division is charged with ensuring that NCIS's program keeps pace with technology acquisition and infrastructure development within the Navy. The Training² Division supports the DoD-wide computer investigations training program.

In 1992, NCIS established a counterintelligence program focused on counterintelligence support to defense against information warfare and counterintelligence activities in an automated environment. This program works closely with NCIS science and technology protection in ascertaining automated threats to the Navy's priority programs. It also actively supports the direction of the NCIS CIO.

In June 1996, NCIS obtained permission from the developer of a shareware program to distribute it free of charge to everyone in the Department of Defense in a modified version entitled, "Protecting Your Children in Cyberspace." This software is a windows-based program which searches hard drives and removable disks for the presence of 30 types of graphics images. It then displays them in miniature by location. The software gives parents the opportunity to see what graphic images have been downloaded to their computers and evaluate, in the privacy of their own home, the impact on their family. NCIS has given away more than 10,000 copies of the software and also uses it to analyze seized computers for evidence in child pornography cases.

¹ The process of taking specific forensic steps, while maintaining the integrity of data and not tampering with potential evidence, to analyze and extract evidence from computer hardware and software.

² On February 10, 1998, the Deputy Secretary of Defense signed a memorandum authorizing Defense Reform Initiative #27 that directed the Air Force to establish a joint DoD Computer Forensics Laboratory and Training Program. The training program is to be supported by all the DCIOs and associated Agencies and will provide computer investigation training to individuals and DoD elements to ensure Defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities. It will have eight basic and advanced courses, will develop capability to train at remote locations, and will develop training that can be provided without instructors.

Description of Computer Investigation Programs

As part of a proactive crime prevention effort focusing on technology, NCIS Special Agents provide computer-related briefings and training to Navy and Marine Corps information systems administrators, military personnel, and military family groups. The briefings provide basic information on technology, threats, and guidelines to minimize potential victimization. The briefings give audiences the opportunity to exchange information with the agents. The agents also provide brochures which contain crime prevention tips. In April 1996, NCIS started a Computer Crime Prevention Hotline.

Air Force. The AFOSI computer crime investigation (CCI) program commenced in the late 1970s when AFOSI trained computer technicians as Special Agents. At that time, the investigations primarily focused on mainframe computers. In the late 1980s, use of desktop computers for criminal activity emerged. At that point, AFOSI began looking at ways to save evidence from these machines. This became the beginning of its computer forensics program. In the early 1990s AFOSI became aware that hackers had begun targeting Air Force computers. Notably, hacker intrusion attempts have increased greatly in recent years due to the rise in internet access and the fact that Air Force computer systems are becoming tied into the internet. AFOSI sees most computer intrusion problems associated with its unclassified systems. Through use of encryption and firewalls, Air Force classified systems are well protected and have not been subjected to significant intrusion attempts.

AFOSI provides support in counterintelligence matters that involve computer crimes to the Ballistic Missile Defense Organization, Defense Security Assistance Agency, Defense Legal Services Agency, Washington Headquarters Services, and the Office of the Secretary of Defense.

AFOSI's CCI program is staffed with agents in the field who are devoted solely to investigations of crimes using and involving computers. At AFOSI headquarters, the CCI program has an attorney from the Office of the Judge Advocate General, computer technicians, forensic specialists, and agents to assist field elements on an ad hoc basis. The CCI agents work by geographic area assignments.

While AFOSI tracks computer crimes cases by a specific category code, AFOSI does not include theft of computers as a computer crime. The primary types of computer crimes cases, other than intrusions, involve pornography, counterintelligence, and espionage. About half of the identified instances of pornography on Air Force computers involve children. AFOSI actively pursues child pornography cases. The other cases involving pornography AFOSI defers to the Security Police or installation Inspector General for action. In FY1997, 40% of the general crimes cases to which the AFOSI laboratory provided forensic support involved child pornography. AFOSI will provide ad hoc support to local installations with a CCI augmentee to assist in media analysis and search and seizures. In recent years, AFOSI has seen growth in counterintelligence and espionage cases that involve computers. In FY1997, the laboratory provided forensic analysis on 8 cases that involved counterintelligence matters.

Computer intrusion cases are handled somewhat differently due to the differences in venue and technical issues. The Intrusion Branch presently consists of 4 agents and 3 technicians. They provide national oversight, coordinate with other law

enforcement agencies, assist agents in the field, and provide media analysis to the field agents.

The Air Force uses the Automated System Information Monitor (ASIM) which operates "real time" at most Air Force bases. ASIM is a computer that watches for typical hacker activities and prints paper records of the actions taken. The Air Force Computer Emergency Response Team, located at Kelly AFB, TX, reviews ASIM print outs. When a suspect activity is identified, it is referred to AFOSI, which has assigned 1.5 staff years to the Computer Emergency Response Team. About 47% of AFOSI's intrusion cases result from alerts by ASIM, 43% from computer systems administrators, and 10% from other human sources.

AFOSI has developed a hardware and software system, nicknamed "Sniffy," which fine tunes the monitoring that ASIM provides. Sniffy is resident on laptop computers and can be installed at the point where an intrusion is attempted to monitor further activity. Sniffy then permits monitoring from an off-site location, usually AFOSI headquarters. To comply with federal wiretap statutes, however, AFOSI must have a court order or the consent of the user to use Sniffy. When possible, AFOSI uses "banners"³ to obtain consent from hackers.

When an investigation establishes that an intruder is using a series of linked computers which cross jurisdictional boundaries, the investigation will be transferred to and run from headquarters. AFOSI is in the process of issuing a new manual to address specific issues and problems associated with intrusion investigations. AFOSI anticipates that resolving future intrusion cases will require a substantial portion of its CCI resources due to the technical complexity and cross-jurisdictional aspect of these cases.

DCIS. To date, DCIS's computer crimes investigations have been reactive efforts to resolve specific cases, but have not been a part of a systematic approach to criminal investigations in an automated environment. DCIS is in the process of establishing a computer intrusion investigative team to detect computer intrusions. The team will work on-site with technicians at the Defense Information Systems Agency (DISA) to provide 24-hour screening of DoD computer systems to identify intrusions and intrusion attempts. If the affected computer or organization is part of a Military Service, the matter will be referred to the appropriate MCIO for investigation. All other events will be referred to a DCIS field element for investigation. The team will assist DCIS field units in conducting the investigation of the referred matter.

The computer intrusion investigation team will track the status of all initiated investigations, notifying DISA when the case has been closed so that DISA can close "holes" in the affected networks that had been left open to monitor the hacker's activities. Whenever an MCIO or the FBI declines to conduct an investigation based on a referral from the DCIS/DISA team, the computer

³ The Department of Justice Search and Seizure Guidelines describe a warning banner as the text put on a screen when a person logs in or attempts to log into a computer system. The contents identify who the system belongs to, whether the user has any rights to privacy while using the system, whether user activities can be monitored, and what may happen if a user illegally accesses the system. By logging in, the user agrees to the terms of the banner.

Description of Computer Investigation Programs

intrusion investigation team will evaluate the referral for its impact at the DoD level and may initiate an investigation if deemed appropriate.

Additional objectives are for the computer intrusion investigation team to provide assistance as needed to the MCIOs and the FBI on intrusion investigations initiated by those organizations, and to coordinate with the MCIOs to accomplish work overseas on behalf of DCIS-initiated investigations.

DoD Computer Laboratory. Cases that involve extensive media analysis or that affect multiple systems so large that the field investigative units cannot adequately handle them will be referred to the new DoD computer forensics laboratory presently being established at Andrews Air Force Base, MD.

On February 10, 1998, the Deputy Secretary of Defense directed the establishment of the Joint DoD Computer Forensics Laboratory and Training Program, which will be responsible for counterintelligence, criminal and fraud computer evidence processing, analysis, and diagnostics. The training program will provide computer investigation training to individuals and DoD elements to ensure that Defense information systems are secure from unauthorized use, counterintelligence, and criminal activities.

The Air Force was designated as the Executive Agent for the laboratory and training program, and as such, was directed to manage the Navy curricula development, the Army distance learning capabilities, and the Air Force computer forensics laboratory. The DCIOs and associated Agencies were directed to provide staffing and funding for FY1998 and FY1999 start-up costs, to sign a Memorandum of Agreement on a reimbursable basis with AFOSI for FY1998 and FY1999 costs, and to identify funds from their FY2000 budgets to be realigned to the Air Force. The Deputy Secretary's memorandum directed the DoD components to give AFOSI their full cooperation and support.

DCIO Computer Crime Investigative Results.

Tables 1 and 2, below, identify the results and monetary outcomes of cases (UCMJ and non-military Federal criminal statutes) investigated by the DCIOs that involved theft, damage, and destruction of computer hardware and software in which indictments, convictions, sentences, suspensions and debarments were obtained between April 1, 1994, and September 30, 1997, as reported in the Inspector General's Semiannual Reports to Congress. Computer intrusion cases are not included. (The NCIS provided additional statistics, as shown in their comments at Appendix D, that reflects numbers resulting from a difference in definition of computer crimes from that used in the Semiannual Reports.) Table 3 identifies cases investigated by the DCIOs that involved computer intrusions during FY1997.

Description of Computer Investigation Programs

Table 1. Results from General Computer Investigation Cases

<u>DCIO</u>	<u>Indictments</u>	<u>Convictions</u>	<u>Article 15s*</u>	<u>Suspensions</u>	<u>Debarments</u>
DCIS	12	6	0	0	0
CIDC	5	31	12	0	0
NCIS	0	1	3	0	0
AFOSI	16	18	9	1	9
TOTAL	33	56	24	1	9

* Article 15 is the nonjudicial punishment clause of the Uniform Code of Military Justice.

Table 2. Monetary Outcomes from General Computer Investigation Cases

<u>Agency</u>	<u>Criminal</u>	<u>Administrative</u>	<u>Seizures/Recoveries</u>
DCIS	\$ 6,350	\$ 3,845	* \$223,102,231
CIDC	0	0	82,045
NCIS	3,025	2,181	11,680
AFOSI	37,850	585	277,523
TOTAL	\$ 47,225	\$ 6,611	\$ 223,873,479

* \$218,000,000 is the value of stolen software recovered in one case.

Table 3. DCIO Computer Intrusion Cases in FY1997

<u>DCIO</u>	<u>Cases Opened</u>	<u>Subject Identified</u>	<u>Action Taken</u>
DCIS	1	0	0
CIDC	7	1	0
NCIS	69	6	2
AFOSI	34	7	2

Resourcing of Computer Investigation Programs

This section addresses budget, personnel, and training provided by each of the DCIOs for investigation of computer crimes. By the end of FY1998, USACIDC will have 22 full-time personnel assigned to its computer crimes program; NCIS 35, AFOSI 64, and DCIS 13. In addition, all DCIOs have agents assigned in the field who have received advanced computer training, but who are not assigned full-time to computer crimes cases. For FY1998, AFOSI budgeted nearly \$3.9 million in support of its program, of which about a third is for conversion to the DoD computer forensics laboratory. DCIS and NCIS computer crime investigation program budgets are contained within their headquarters budgets and were not delineated for FY1998. NCIS proposed \$3.5 million in mid-year 1998, which includes cost of upgrading space for its computer unit. USACIDC estimated its startup costs at \$442,000 for FY1998. Training for agents is consistent among the DCIOs and relies heavily on FLETC or equivalent courses for field agents, supplemented by training available from other law enforcement and computer training sources.

Personnel

Army. USACIDC's CCIT team is located at the LIWA and consists of 4 military billets (2 warrant officers and 2 enlisted members) and one civilian programmer or analyst. In February 1998, only two of the military slots were filled, but USACIDC anticipates filling the remaining two military billets by summer 1998. Filling the analyst slot will require an unknown time to comply with civilian hiring regulations. The Office of the Staff Judge Advocate provides a legal advisor to the USACIDC program.

By summer 1998, each of USACIDC's twelve districts worldwide will dedicate one special Agent to monitor computer crime investigations within the district.

USACIDC operates its Criminal Investigations Laboratory at Ft. Gillem, Georgia. The laboratory has one computer forensic examiner presently on its staff and announced a second civilian position in April 1998. The lab examiners provide technical information in support of affidavits for search warrants involving computer crimes, serve as expert witnesses, conduct high-level forensic examination of computer media and hardware, provide real time assistance to field investigators, and provide on-scene assistance to investigators for crimes involving computers.

Navy. As presently structured, the Computer Investigations and Operations Department is headed by a GS-15 Deputy Assistant Director. Six NCIS special agents, one U.S. Marine Corps Criminal Investigation Division Special Agent,

one computer specialist, one analyst, and one support person are assigned at headquarters. NCIS has 10 field Special Agents assigned full-time to computer crimes investigations. In addition, NCIS has five agents assigned full-time to the FIWC.

NCIS anticipates filling 11 vacancies in FY1998, and plans to recruit an additional 30-34 people in FY1999 and 30 in FY2000, to bring their end strength to 90-94 people by the year 2000.

Air Force. AFOSI has 64 billets in its CCI program of which 47 are agents and 17 active duty support personnel. Twelve agents are civilians; the balance are active duty. All support personnel are active duty. Of the agents, 2 are assigned to the AFOSI Academy; 32 are located in field detachments; and 13 are assigned to Headquarters, the forensics laboratory, or to the intrusion team currently located in Crystal City, Virginia. Of the support personnel, 8 are assigned to the laboratory and 6 to the intrusion team. The remaining three consist of an attorney, a requirements specialist, and a logistics specialist. As of February 1998, AFOSI has 62% of its billets filled. They have identified individuals to fill most of the empty slots and are striving to have the personnel trained and on board by the end of calendar year 1998.

DCIS. Currently, DCIS has one GS-14 as the Director, Computer Crimes Programs, at Headquarters, one GS-13 agent, and one GS-13 detailed to support the program for 90 days. On April 2, 1998, DCIS announced five position vacancies for its computer intrusion investigative team. The announcement will remain open until all positions are filled. In addition, DCIS anticipates hiring three GS-1801 investigators, two forensic analysts, and an investigative review assistant to complete their computer intrusion investigative team.

Budget

Army. USACIDC estimates that the startup costs of its CCIT will be about \$200,000 for hardware, software, training, office equipment, and temporary duty travel. Salaries account for an additional \$242,000. Hardware and software resources will be centrally procured and controlled by CCIT to maintain standardization, and will be distributed to the District Coordinators when needed. Emergency needs will be coordinated by CCIT.

Navy. The NCIS CIO budget is contained within the overall NCIS headquarters budget. They have submitted a midyear FY1998 proposal to obtain a separate \$3.5 million budget. If approved, the funds would include the cost of upgrading the physical operating space for the CIO.

Air Force. For FY1998, AFOSI has budgeted \$2,856,500 in support of its computer crime investigation program. Of this amount, \$1.3 million is for the conversion of AFOSI's laboratory into the DoD computer forensic laboratory. As of February 28, 1998, the \$1.3 million had nearly all been expended. Of the remainder, the CCI program has budgeted \$565,000, more than half of which covers the cost of temporary duty for its counterintelligence and detachment specialists. An additional \$180,000 is allocated for contract support, which

Resourcing of Computer Investigations Programs

includes training. Communication devices, computer stations for administrative personnel, and local purchase monies account for \$35,900. Finally, AFOSI Headquarters has allocated \$1 million for research and development. Half is allotted for development of work stations for technicians and the remainder for developing a way to detect and counteract steganography--transmission of documents hidden in an electronic picture or sound file.

After FY1998, AFOSI expects its research and development budget to be about \$500,000 per year. The Defense Reform Initiative will provide additional monies to the forensic laboratory through financial support transferred from other agencies. AFOSI anticipates that the laboratory's total FY1999 budget will be at least \$2.5 million.

DCIS. The costs associated with the DCIS computer intrusion investigative team are included as part of the overall headquarters budget and are not delineated separately.

Training

Army. USACIDC delineates four levels of training for computer crimes investigators:

All general field agents will receive a 1-day introduction to computers that provides basic understanding of computer use and potential forms of evidence obtained from computers, and a 2-day course in processing automated crime scenes. This course identifies types of computer networks, forms of computer media storage, discussion on seizing computers and computer media, preservation of evidence, legal issues, current federal and state laws pertaining to computer involved crimes, and preparation and execution of search warrants for computers and computer-related media.

The advanced field agents located at each of the districts will attend the 2-week FLETC course, "Criminal Investigations in an Automated Environment Training Program," and local area network (LAN) training. A source for the LAN training has not yet been identified, but the subject matter covered will include an understanding of network architectures, network software, locating files and data on networks, and seizures of LANs.

CCIT agents will complete the FLETC "Seized Computer Evidence Recovery Specialist" (SCERS) course (2-weeks), and a variety of other courses, sources for which have not been finalized. These include training offered by the International Association of Computer Investigative Specialists, LAN training, Windows NT Basic and Security courses, UNIX Operating System courses (basic and advanced), and various courses addressing investigations involving the internet. Since FLETC does not offer any training in Macintosh or UNIX, the latter courses may be available from the Navy at 29 Palms, California. Two CCIT agents will receive Microsoft and Novell Certified Network Engineer Training.

USACIL examiners receive the FLETC "Computer Evidence Analysis Training Program," SCERS, and a 2-week course offered by the International Association

of Computer Investigators. In addition, USACIL examiners will take a self-paced training available on compact disks offered by Novell, Microsoft and A+. To stay current on technology they will receive an annual, one-week International Association of Computer Investigators update and every three years will retake SCERS.

In addition to FLETC and Navy courses, mentioned above, USACIDC has available as training sources the Army Military Police and Military Intelligence Schools, AFOSI computer training courses, and GSA schedule courses from The Learning Tree. USACIDC is also considering using other sources, such as Army Reservists who have specialized computer knowledge, to provide specialized training to agents as part of their active duty tours.

Navy. Almost all CIO personnel have successfully completed some of the seven computer crime classes currently offered at FLETC. Additional training has been completed by several CIO members in UNIX operating systems, and the International Association of Computer Investigations Specialists, both two-week training programs. NCIS sponsored a UNIX System Administrators for Law Enforcement course at 29 Palms, California, in March 1998, and nearly all CIO personnel have completed this training. CIO, with the Federal Bureau of Investigation, sponsored a one-week Macintosh training course offered in March 1998 at NCIS headquarters. NCIS sets no limits on the amount of training time or quantity of courses computer investigation specialists may take.

In the Spring of 1996, NCIS was chartered to participate, as co-chair, in an OSD working group on computer crime. This working group led to the development of a DoD wide computer forensics and computer investigations training facility. Initially, NCIS was designated executive agent for the training program while AFOSI was executive agent for the computer laboratory. With the implementation of Defense Reform Initiative Directive 27, these efforts were combined under an Air Force Executive Agency, which incorporates the original work by NCIS in this ongoing effort. A senior special agent has been detailed to AFOSI as director of the training program. This dynamic program will meet the needs of each of the DCIOs and support the needs of other computer professionals. Future NCIS training will rely heavily upon the Defense Computer Training Facility.

Air Force. AFOSI's long term training plan for its CCI staff is three-tiered. Tier I consists of 4 weeks of basic training for all CCI staff during their first year as specialists. Tier II, usually accomplished during the second year of a CCI staff member's assignment, will include courses in advanced networking, information systems operations, and counterintelligence collections and investigations. Tier III courses, to be offered in the third year and thereafter, have not been fully identified, but will be designed to meet specialized needs, such as counter-espionage operations. Tier III courses may be developed and/or operated through a contractor.

Since 1993, AFOSI has trained its CCI staff with a one-week course that teaches the basics of how to search a computer disk. Most of its current staff have had only this course. Beginning March 1998 and continuing quarterly for two years, AFOSI began presenting a new two-week Computer Forensic Field Examination course to teach more advanced media analysis techniques for its computer

Resourcing of Computer Investigations Programs

specialists. This course is similar to the "Criminal Investigations in an Automated Environment" course taught at FLETC and is being developed because AFOSI has not been able to acquire sufficient slots to train its staff at FLETC. Each AFOSI course will accommodate 16 students; by the end of FY1999, AFOSI anticipates that all CCI staff will have received this training course.

Specialists will receive a more technical, 2-week course, commencing May 1998. This course is being co-developed with the Federal Bureau of Investigation and will teach more advanced media analysis techniques. AFOSI is also in the process of developing a follow-on course, "Computer Forensic Laboratory Examiner," which all new lab examiners and CCI staff will attend.

Long term plans for AFOSI training include a teaching curriculum being developed by NCIS. Both the curriculum and classroom space are funded through the DoD initiative directed by the Deputy Secretary of Defense. AFOSI anticipates that the curriculum will be operational by FY1999 or FY2000.

DCIS. DCIS sends selected field agents to FLETC for two week training at the "Criminal Investigations in an Automated Environment" and SCERS courses. A total of 40 agents have received "Criminal Investigations in an Automated Environment" training from FY1995 through FY1998 to date, and 13 have received the advanced SCERS training during the same time period.

By the end of FY1999, DCIS plans to have 50 of its field agents trained to handle referrals made by the DCIS/DISA computer intrusion team. The week-long training will emphasize procedural handling of referrals rather than technical aspects of computer crimes investigations that are available from FLETC.

Program Concerns

A concern of all the DCIOs is the recruiting and retention of qualified, experienced agents to conduct computer crimes investigations due to competition with the private market and the high salaries that can be commanded by capable technicians. Also cited as concerns that affect the ability of individual DCIOs to be effective in the conduct of computer intrusion investigations were: constant training to keep up with technology and hacker activities, lack of timely notification of intrusions, capability of maintaining real-time monitoring of Departmental systems, lack of physical space for storage of hardware and software, lack of ability to measure results of intrusion investigations, and lack of management support within the Department.

Recruiting and Retention

USACIDC prefers to employ military instead of civilian agents, especially those who are new Warrant Officers or those who have recently reenlisted because the military can retain them longer. USACIDC is also planning to use recent military graduates of the Army education program as a method of retaining trained specialists since the education program commits the recipients to a minimum of three more years service. In the future, if the Army recognizes Information System Management as a degree for which it will authorize educational funding, USACIDC will send selected Special Agents to civilian schools to obtain the degree in exchange for a 3-year duty obligation for each year of education the agents receive. Recruiting difficulties are illustrated by USACIL's recent cancellation of an announcement for a GS-12 forensic examiner after receiving only two applications. USACIL is reissuing the announcement as a GS 9/11/12 hoping to receive more applications, primarily from recent college graduates.

Until lately, recruiting capable people for the AFOSI program was a problem. Communications specialists had to be released from their occupational field to serve in AFOSI and then returned to their field at the end of their AFOSI assignment. AFOSI has recently arranged with the Air Force personnel system to get "first cut" of active duty specialists and to retain them in AFOSI instead of having to release them to the communications field after their tour of duty with AFOSI. Since the inception of its program, AFOSI has attempted to recruit officers who obtain computer science degrees as they graduate from college or the Air Force Academy. In addition, AFOSI is now seeking new CCI specialists from the Staff and Technical Sergeant ranks. These individuals usually have 13-15 years of active duty and are more likely to remain in the Air Force until retirement, thereby potentially giving 5 or more years to AFOSI once they have been trained as CCI specialists.

AFOSI considers retention of trained computer investigative specialists a serious problem. On the average, civilian specialists put in one 2 to 4 year tour and then are lost to private industry or other Federal government agencies that offer higher

salaries. Active duty communications specialists also leave AFOSI in order to assume responsibilities as a detachment commander in order to be promoted.

In April, DCIS began the process of staffing its computer intrusion investigative team by announcing multiple criminal investigator vacancies. The DCIS Program Director was uncertain how successful they would be recruiting against private industry, which pays substantially more than a GS-13 salary for experienced workers. The personnel specialist servicing the announcement confirmed that almost none of the applicants to date had the requisite computer background.

Training

AFOSI acknowledged that due to the rapidly changing nature of cyberspace technology, new hardware and software, and the manner in which hackers operate, technicians and specialists must constantly receive training to stay current with the changes and legal developments that affect criminal investigations.

Timeliness and Time Constraints

USACIDC has noted a lack of prompt notification (within 24 hours) by Army commands of computer intrusions. The establishment of the liaison function between CCIT and LIWA was undertaken to improve this factor.

AFOSI noted that its field agents spend over 25% of their time doing media analysis. AFOSI wants to eliminate this burden on field agents by either having technicians at headquarters do the analysis, by having a specialized augmentee at each detachment capable of providing that service, or by having each detachment contract for the service. By reducing the time agents spend doing media analysis, agents will be able to concentrate on the remaining investigative steps necessary to complete the case, for which they are specially trained.

Hardware, Software, and Space

NCIS noted that they must have a duplicate set of equivalent hardware and software in order to analyze seized computers and related data stored on various types of media, including everything from old Commodore and Radio Shack computers to state-of-the-art equipment. Analysis can be performed using the duplicates, thereby avoiding the risk of alteration, damage, or loss of evidence during the process. Duplicate equipment is expensive and requires proper storage space to keep it operationally ready even when not in active use. NCIS acknowledged that when they do not possess hardware or software to perform analysis in a particularly case, they try to borrow what is needed from another law enforcement agency. An additional problem is the need to train agents on proper use of the variety of software and hardware during the analysis process.

salaries. Active duty communications specialists also leave AFOSI in order to assume responsibilities as a detachment commander in order to be promoted.

In April, DCIS began the process of staffing its computer intrusion investigative team by announcing multiple criminal investigator vacancies. The DCIS Program Director was uncertain how successful they would be recruiting against private industry, which pays substantially more than a GS-13 salary for experienced workers. The personnel specialist servicing the announcement confirmed that almost none of the applicants to date had the requisite computer background.

Training

AFOSI acknowledged that due to the rapidly changing nature of cyberspace technology, new hardware and software, and the manner in which hackers operate, technicians and specialists must constantly receive training to stay current with the changes and legal developments that affect criminal investigations.

Timeliness and Time Constraints

USACIDC has noted a lack of prompt notification (within 24 hours) by Army commands of computer intrusions. The establishment of the liaison function between CCIT and LIWA was undertaken to improve this factor.

AFOSI noted that its field agents spend over 25% of their time doing media analysis. AFOSI wants to eliminate this burden on field agents by either having technicians at headquarters do the analysis, by having a specialized augmentee at each detachment capable of providing that service, or by having each detachment contract for the service. By reducing the time agents spend doing media analysis, agents will be able to concentrate on the remaining investigative steps necessary to complete the case, for which they are specially trained.

Hardware, Software, and Space

NCIS noted that they must have a duplicate set of equivalent hardware and software in order to analyze seized computers and related data stored on various types of media, including everything from old Commodore and Radio Shack computers to state-of-the-art equipment. Analysis can be performed using the duplicates, thereby avoiding the risk of alteration, damage, or loss of evidence during the process. Duplicate equipment is expensive and requires proper storage space to keep it operationally ready even when not in active use. NCIS acknowledged that when they do not possess hardware or software to perform analysis in a particularly case, they try to borrow what is needed from another law enforcement agency. An additional problem is the need to train agents on proper use of the variety of software and hardware during the analysis process.

DCIS noted that computer intrusion monitoring equipment is very costly. DCIS plans to interface with DISA and use their hardware, software, and specialists to track intrusion cases. This will reduce operating costs by maximizing the use of available DoD resources.

Measuring Results

The Army has no standard against which to compute loss suffered as a result of computer intrusions. USACIDC measures the "solve rate" of its cases, and considers intrusion cases an investigative "success" when a hacker/cracker has been identified and prosecuted, or when they establish that no crime occurred.

NCIS continues to improve its performance in the resolution of computer related crimes and is currently developing investigation resolution based-metrics for continued response to the Department of the Navy.

AFOSI cases have generally not resulted in jail time for perpetrators convicted of computer crimes. However, identification of the hacker often leads to acquisition of the software the hacker used to effect intrusion. From that, AFOSI agents can learn what hackers are doing and their motivation for doing so. They also evaluate the hacker's software for counterintelligence impact and whether hackers were working alone or with other people. While extremely important from an operational point of view, AFOSI has not developed an effective method for measuring this type of data.

DCIS noted that capturing data about computer crime investigations depends on how the case is categorized in its database. As an example, DCIS opened a case on a Government official suspected of accepting bribes. During a search of the official's Government computer, they discovered child pornography images for which the official was later convicted. This case could have been categorized as a computer-type crime since the computer was used in the transfer and storage of the illegal images, but it remained in the database as a bribery case. Thus, a search of the database by category code would not count this case when the query is restricted to computer crimes.

Programmatic Support

As mentioned above, USACIDC has noticed a lack of awareness by local Army commands concerning the negative impact of computer intrusions and the importance of notifying LIWA of all intrusion attempts. When the Army completes the unification of its network, systems management, and security functions, this issue may diminish.

As the Department of Navy continues to recognize the value of technology based information dissemination and enhanced decision making capability, NCIS is moving to meet this new mission area. The technological *Defense in Depth* strategy must include integrated law enforcement, counterintelligence and

security support to offset "insider" threats as well as the continuous external threat to the information systems.

Conclusion

The DCIOs recognize the necessity of having specially trained agents to handle equipment seizures, technical analysis of computers, and identification of intruders. While CID, NCIS, and DCIS's programs are in their relative infancy, AFOSI has had an established program for over 15 years. The Air Force laboratory is soon to assume the role as the DoD computer crime laboratory. Retention of quality technicians and adequate funding during DoD downsizing are significant challenges to the investigation of computer intrusions and fraud against the DoD that involve the use of computers.

Part II - Additional Information

Appendix A. Individuals Visited or Contacted

- Army: Sidney Younger, Chief, Fraud Division, USACIDC
Jon Woodman, Policy Staff Officer, USACIDC
Paul Constable, Chief, Policy, USACIDC
Jeffrey Porter, Headquarters, Department of Army, Military Police
Operations Branch
Daniel Quinn, Deputy Chief of Staff for Operations, USACIDC
Jeffrey Hormann, Chief, CCIT, Field Investigative Unit,
USACIDC
Willie Rowell, Chief, Current Operations,
Headquarters, USACIDC
Raymond Miller, Chief, Internal Review Office, USACIDC
James Pace, Computer Investigations Specialist, USACIL
- Navy: Matthew Parsons, Special Agent, CIO, NCIS
Daniel Gray, Special Agent, CIO, NCIS
- Air Force: Ann Burt, Program Manager, CCI Program, AFOSI
David Morrow, Former CCI Program Manager, AFOSI
Robert Walker, Policy Officer, AFOSI
- IG, DoD: Jane Charters, Director, Investigative Support Directorate, DCIS
John Gosser, Program Director, Computer Fraud Program, DCIS
Robert Hodge, Assistant Director, Information Management and
Analysis Division, DCIS
Mark Spaulding, Assistant Director, Special Operations
Programs, DCIS
Claudia Gander, Investigative Support Specialist, DCIS
David Botsko, IG Representative, FLETC, Brunswick, GA
Christine Heredia, Personnel Staffing/Classification Specialist,
Office of Assistant Inspector General for Administration and
Information Management

Appendix B. Summary of Prior Evaluations

General Accounting Office

“Information Security Management, Learning from Leading Organizations” November 1997, Report No. GAO-AIMD-98-21. This guide studied organizations with reputations for having superior security programs and identified practices that could be adopted successfully by federal agencies to better manage information resources.

“Information Security--Computer Attacks at Department of Defense Pose Increasing Risks,” May 1996, Report No. GAO/AIMD-96-84. GAO reported that Department of Defense computer systems are increasingly attacked by hackers who have stolen, modified, or destroyed data and software, installed unwanted files and “back doors” which circumvent normal system protections, and seized control of entire systems that support critical functions such as weapons system research, logistics, and finance. The report recommended that the Department develop policies for preventing, detecting, and responding to attacks; require the Military Services and Defense Agencies to use training and other mechanisms to increase awareness and accountability among installation commanders to security risks; develop department-wide network monitoring and protection technologies; evaluate incident response capabilities to ensure they are sufficient to handle the projected threat; and assign responsibility and accountability to ensure successful implementation of a computer security program.

Inspector General, DoD

“Computer Security for the Federal Acquisition Computer Network,” August 22, 1996, Report No. 96-214. The audit evaluated procedures for data security, continuity of operations, transaction audit trails, personnel security, and compliance with security requirements for small purchases made through the electronic commerce and electronic data interchange program between the Government and its contractors. The Federal Acquisition Streamlining Act of 1994 requires the development of the Federal Acquisition Computer Network. The audit found that the Defense Information Systems Agency had not obtained capabilities for digital signatures or encryption for procurement transactions over the system, that there were no established data backup procedures to ensure recovery from data disasters, and that the system did not adequately control access to protect it from fraud and criminal threats.

“Computer Security Over the Defense Joint Military Pay System,” June 25, 1996, Report No. 96-175. The audit evaluated whether controls were adequate to limit application access to authorized employees and to limit authorized users to programs, functions, and data required to perform their duties in managing the

Appendix B. Summary of Prior Evaluations

joint payroll system for the Army and Air Force. The audit found that application resources were not secure; the integrity of pay data was at risk; responsibilities for authorizing and controlling access to the system were not clearly defined and understood at some sites; and security oversight was inadequate.

Army Audit Agency

“Army Web Server Security,” January 20, 1998, Report No. AA 98-10. The audit evaluated the Army’s Homepage registration and web server security certification processes, assessing to what extent internet security concerns were addressed through training and awareness programs. It found that the Army’s current policies and procedures provide some assurance that Privacy Act and other sensitive, unclassified information is protected from unauthorized access and disclosure. However, policies do not adequately identify or address network security risks associated with connecting a web server to the internet; personnel assigned as web managers are not always trained on information systems security; the Army has not established a formal training program for web managers; and the Army has not developed comprehensive guidance to increase the awareness of personnel and contractors who use Army computer resources to access the internet.

“Information Systems Security Program,” June 30, 1997, Report No. AA 97-214. The audit examined the operational and electronic aspects of the Army’s Information Systems Security Program and evaluated to what extent unclassified, sensitive sustaining base networks and information systems were vulnerable to attack. The audit found the systems were highly vulnerable to malicious attack, exploitation, compromise, denial of service, and sometimes destruction by computer hackers. The vulnerabilities existed because automated security controls were not adequate or were not adequately used, alignment of information security responsibilities did not effectively integrate systems operations; security specialists and system administrators did not use effective practices and procedures to identify and assess operational safeguards and measures; and controls did not exist to hold commanders accountable for maintaining secured information infrastructures and measure whether the security program was achieving intended security outcomes.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Assistant Secretary of Defense (Command, Control, Communications & Intelligence)
General Counsel, DoD
Director, Defense Criminal Investigative Service*

Department of the Army

Auditor General, Department of the Army
General Counsel of the Army
Commander, U.S. Army Criminal Investigation Command*

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
General Counsel of the Navy
Director, Naval Criminal Investigative Service*
Counsel for the Commandant (Marine Corps)

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
General Counsel of the Air Force
Commander, Air Force Office of Special Investigations*

* Recipient of draft report.

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Part III – Management Comments

Part III – Management Comments

Department of the Army Comments

Final Report
Reference



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
8010 6TH STREET
FORT BELVOIR, VA 22060-8266

CIOP-PO

15 JUL 1988

MEMORANDUM FOR Department of Defense Inspector General,
ATTN: CIPO, 400 Army Navy Drive,
Arlington, VA 22202-2884

Subject: Review of Draft DoDIG Report (Evaluation of Defense
Criminal Investigative Organization Programs for Investigating
Computer Crimes)

1. The draft report concerning the above subject matter was
reviewed. The following comments are provided for your
consideration:

a. Page ii, top paragraph: The start-up costs for the
USACICD should read \$442,000 as stated on page 12.

b. Page 4, remainder of last paragraph from page 3: The
Computer Crimes Investigation Team (CCIT) is not responsible for
writing and disseminating policy for the USACICD. Policy is
published at the headquarters level and a subordinate unit such
as the CCIT will recommend and review policy.

c. Page 4, first paragraph: The district coordinators will
review crime prevention surveys, not conduct them. Additionally,
the coordinators will ensure computer crime awareness briefings
are accomplished, not necessarily provide them. The district
coordinator supervises and monitors the activities of subordinate
offices.

d. Page 12, Army, first paragraph: The CCIT is not located
at Headquarters, USACICD. It is located at the Land Information
Warfare Activity (LIWA) and is subordinate to the Field
Investigative Unit (FIU), which is subordinate to the
701st Military Policy Group, USACICD.

e. Page 12, Army, second paragraph: The paragraph reads,
"By summer 1998, each of USACICD's twelve districts worldwide
will dedicate one special agent to conduct..." and the word
"conduct" should be replaced with "monitor" since the district's
responsibility is to supervise subordinate investigative units.
The goal is to have a minimum of one agent trained to investigate
computer crimes at each investigative unit.

Exe Sum
Page i

Page 4

Page 4

Page 11

Page 11

Printed on Recycled Paper

CIOP-PO

Subject: Review of Draft DoDIG Report (Evaluation of Defense
Criminal Investigative Organization Programs for Investigating
Computer Crimes)

2. The point of contact is CW4 Paul D. Constable, 806-0219,
fax 806-0220, or email constablep@cidc.belvoir.army.mil.

FOR THE COMMANDER:



DANIEL M. QUINN
Colonel, GS
Deputy Chief of Staff
For Operations

Department of the Navy Comments

DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
Washington Navy Yard Building 111
716 Secord Street South East
WASHINGTON, DC 20388-5380

5100
8205-1/BAN
24 July 1998

From: Director, Naval Criminal Investigative Service, Washington Navy Yard,
Washington DC 20388-5380
To: Deputy Assistant Inspector General, Criminal Investigative Policy and Oversight,
Office of the Inspector General, Department of Defense, Washington, DC
Subj: EVALUATION REPORT ON DEFENSE CRIMINAL INVESTIGATIVE
ORGANIZATION PROGRAMS FOR INVESTIGATING COMPUTER
CRIMES

Encl: (1) NCIS Comments for Project No. 70G-9022

1. We forward the enclosure as our comments to your draft Evaluation Report.
2. We thank you for the opportunity to review the draft and look forward to providing you with additional information in your ongoing evaluation of Defense Criminal Investigative Organizations (DCIO) programs for investigating crimes affecting computers and computer systems.
3. If you have any questions, please do not hesitate to contact Special Agent Alexander P. Zane, Deputy Assistant Director for Computer Investigations and Operations at 202.433.9275. or at azane@ncis.navy.mil.

(Original signed)
A. P. ZANE

Final Report
Reference

NCIS Comments for Project No. 70G-9022: Evaluation of Defense Criminal Investigating Organization Programs for Investigating Computer Crimes

Description of Computer Investigation Programs (page 5)

Insert as paragraph 1 under Navy.

NCIS views "Computer Crime" as those cases which include computers being used as the means or tool to commit an offense; a repository for data or other evidence of an offense; or as the target of an act which affects the confidentiality, integrity or availability of sensitive data or network communications. Investigative considerations by NCIS include the theft, damage or destruction/corruption of hardware or software where the computer is the sole target of the offender. (Example: A command may report the theft of a laptop computer as a relatively minor monetary loss, but to NCIS the value of the information stored on the computer may be significantly higher from a classification, proprietary, economic or access perspective.)

Page 5

Insert as paragraph 3, after "... administrative support by the Navy and Marine Corps to victims."

Page 6

In 1992, NCIS established a counterintelligence program focused on CI Support to Defense against Information Warfare and CI Activities in an Automated Environment. This program currently works closely with NCIS Science and Technology protection in ascertaining automated threats to the Navy's priority programs. It is also actively supporting the direction of NCIS CIO.

For inclusion into Table 1: "Results from General Computer Investigation Cases

	Indictments	Convictions	Article 15	Suspensions	Debarments
NCIS	51	25	13	2	2

Not
Changed

For inclusion into Table 2: "Monetary Outcomes from General Computer Investigation Cases"

	Criminal	Administrative Seizures/Recoveries
NCIS	\$594,990	Unavailable \$647,948

Not
Changed

For inclusion into Table 3: "DCIO Computer Intrusion Cases in FY 1997"

	Cases Opened	Subject Identified	Action Taken
NCIS	69	6	2

Page 10

Personnel (page 13)

Delete: As presently structured, the "Computer Crime Investigations Support Unit"

Insert: As presently structured, the "Computer Investigations and Operations Department"

Page 12

Training (page 16)

Navy. Almost all CIO personnel have successfully completed some of the seven computer crime classes currently offered at FLETC. Additional training has been completed by numerous CIO members including UNIX operating systems, and the International Association of Computer Investigations Specialists, both two-week training programs. NCIS sponsored a UNIX System Administrators for Law Enforcement course at 29 Palms, California in March 1998, and nearly all CIO personnel have completed this training. CIO, with the Federal Bureau of Investigation, sponsored a one-week Macintosh training course offered in March 1998 at NCIS Headquarters. NCIS sets no limits on the amount of training time or quantity of courses computer investigations specialists may take.

Page 14

In the Spring of 1996 NCIS was chartered to participate, as co-chair, in an OSD working group on computer crime. This working group has led to the development of a DoD wide computer forensics and computer investigations training facility. Early on NCIS was the designated executive agent for the training program while AFOSI was executive agent for the computer laboratory. With the implementation of Defense Reform Initiative Directive (DRID) 27, these efforts were combined under an Air Force Executive Agency, which incorporates the original work by NCIS into this ongoing effort. A senior special agent has been detailed to AFOSI as director of the training program. This dynamic program will meet the needs of each of the respective DCIOs and support the needs of other computer professionals. Future NCIS training will rely heavily upon the Defense Computer Training Facility.

Page 14

Measuring Results (page 21)

Delete paragraph starting with: "NCIS is improving..."

Final Report
Reference

Page 19

Insert: NCIS continues to improve its performance in the resolution of computer-related crimes and is currently developing investigation resolution-based metrics for continued response to the DoN.

Programmatic Support (page 21)

Delete paragraph starting with, "NCIS wants Navy..."

Page 20

Insert: "As the Department of the Navy continues to recognize the value of technology based information dissemination and enhanced decision making capability, NCIS is moving to meet this new mission area. The technological *Defense in Depth* strategy must include integrated law enforcement, counterintelligence and security support to offset "insider" threats as well as the continuous external threat to the information systems."